Gröbner bases and Standard bases

Broer, H.; Hoveijn, I.; Lunter, G.; Vegter, G.

Published in:
EPRINTS-BOOK-TITLE

6 Gröbner bases and Standard bases

This chapter explains how to compute the codimension of the tangent spaces used in chapters 2 and 3: ideals, and left-right tangent spaces of the form (3.7), both as subsets of the ring of formal power series. For ideals, this can be done by calculating the formal power series equivalent of a Gröbner basis. This idea is generalized and applied to left-right tangent spaces.

6.1 Introduction

A Gröbner basis of an ideal in a polynomial ring is a set of generators with certain additional properties. One implication of these is that a normal form algorithm exists, equivalent to a 'division': Given an arbitrary polynomial, the algorithm expresses it as an ideal element, plus a unique remainder term in a certain minimal vector space. The dimension of this vector space is called the *codimension* of the ideal, which is finite for our application.

That application is Kas and Schlessinger's algorithm, constructing a right transformation inducing an arbitrary unfolding from a versal one. The ideal is related to the versal unfolding's tangent space, whereas the remainder terms are related to the (finitely many) deformation terms. Kas and Schlessinger's algorithm is the subject of Chap. 7.

These ideas need to be generalized somewhat, first of all because the tangent space we consider is not a *polynomial* ideal, but an ideal in the formal power series ring; see Chap. 5. Secondly, in the case of left-right transformations, the tangent space is no longer an ideal. For both of these cases, this chapter develops an appropriate normal form or 'division' algorithm.

Overview The problem of computing the codimension of an arbitrary polynomial ideal I in a polynomial ring R was solved by Bruno Buchberger in his 1965 thesis [Buc65]. His idea was to introduce an ordering on the monomials. The largest monomial occurring in a polynomial, with respect to this ordering, is called its *leading monomial*, and the ideal generated by the leading monomials of ideal members he called the *leading monomial ideal*, written as $\mathsf{LM}\, I$. The number of monomials not in $\mathsf{LM}\, I$ is precisely the codimension of I, i.e., the dimension of R/I as an $\mathbb{R}$-vector-space.

H. Broer, I. Hoveijn, G. Lunter, and G. Vegter: LNM 1806, pp. 97–132, 2003.

We now briefly sketch the main idea. Assume we have generators h_i of I, then clearly multiples of leading monomials of the h_i are in $\mathsf{LM}\, I$, but the converse is not generally true. Buchberger developed an algorithm computing a basis h_i' generating the same ideal I, but with the additional property that their leading monomials do generate $\mathsf{LM}\, I$. Such bases are called Gröbner bases. Gröbner bases are used to systematically solve a number of questions involving polynomial ideals. For some problems occurring in algebraic geometry, see [CLO98, GP88, MR88] and also [CLO92] which gives a good introduction to Gröbner basis theory. Many generalizations have been developed, for example for submodules (see [GP88]), for ideals in power series rings [Bec90a, Bec90b, Hir64, Mor88], and for subalgebras of polynomial rings [AHLM99, KM89, Mil96, RS90, Stu96, Vas98].

One problem in polynomial ideal theory which Gröbner bases solve, and which once was the main problem of the field (see van der Waerden [Wae60], and [Win96]), is the *ideal membership problem*: for a given f, decide whether it is an element of an ideal I. If a Gröbner basis of I is known, there is a *normal form algorithm*, which, for any equivalence class $f+I$ defined by a representative $f \in R$, returns a unique representative of that class. It is clear that this solves the ideal membership problem. A suitably modified version of the algorithm works in the ring of truncated formal power series, and is used in Chap. 7 to obtain reparametrizations and coordinate transformations related to versal unfoldings; see also [BHLV98, Lun99b].

In this chapter those generalizations are brought under a common umbrella. An abstraction is made both of of the base vector space (e.g. the ring of polynomials, truncated formal power series, or rational functions), and the algebraic structure of the set T of interest (ideal, submodule, subalgebra, left-right tangent space). Also the concept of 'monomial' is generalized: For our purposes the key property is not that monomials form an algebra, but that they form a basis of the base vector space (ring, module, algebra).

The algebraic structure is described by a map Ψ whose image is T, and we investigate its monomial structure. If this map satisfies certain properties, it is called a *standard map*. The main implication is that for such maps, the set $\mathsf{LM}\,\mathrm{Im}\,\Psi$ can be described explicitly, and using this, T's codimension can be computed.

The idea for this approach is based on the presentation of Greuel [GP88] for standard bases of submodules. More precisely, the proof of the standard map theorem 6.10 follows Greuel's proof of Schreyer's method for computing the module of syzygies of an ideal, stripped of the algebraic details unnecessary in the general setting. We also use the Schreyer order [Sch91] of monomials, which we call the *induced order* in the general context.

The algorithms for computing standard subalgebra bases, also known as *SAGBI*[1] or *canonical* bases, were taken from Sturmfels [Stu96]. The problems one encounters here are related to integer linear programming. Interestingly,

[1] *S*ubalgebra *A*nalogue of *G*röbner *B*ases for *I*deals, see e.g. [Vas98]

these can be solved using Gröbner bases again (see [CLO98, Ch. 8] and [Sch86, §16.4]). The algorithms to compute standard basis for left-right tangent spaces were based on these techniques, and also involve Gröbner basis calculations.

There are other possibilities for generalizations that are not mentioned yet, see e.g. [CCS99, Ch. 1]. In particular, we shall always assume that the coefficients are elements of a *field*, which avoids a number of complications that are encountered in the case of a base *ring*. For this topic we refer to e.g. [AHLM99, Mil96].

Organization of the chapter First we present the theory of Gröbner bases, without proofs, so as to suggest a generalization. In Sect. 6.3 the abstract setup is given, with the standard map theorem 6.10 underlying the subsequent results. Section 6.4 deals with several instances of standard bases, starting from Gröbner bases, and culminating in standard bases for left-right tangent spaces. The final section is about the differences encountered when these spaces live in the ring of (truncated) formal power series, instead of the polynomial ring.

6.1.1 Algorithms and real numbers

This chapter describes algorithms performing various computations. We here make some remarks how these algorithms are idealizations of their actual computer implementation. More down to earth, it can be regarded an attempt at justifying the use of real and complex numbers in the algorithm descriptions.

Mathematical models of computers, for example Turing machines (see e.g. [Dav65]), are usually discrete. This is reasonable, since modern computers are digital, and have well-defined discrete states. On the other hand, in mathematics we often use the fields $\mathbb{R}$ or $\mathbb{C}$ for computations, and their elements cannot be represented by a discrete model. So, when a mathematician wants to model algorithms performing 'real' calculations on a digital computer, there is a problem.

One solution would be to restrict to so-called *computable* fields, for instance finite fields, see e.g. [BW93]. However, one could also argue that the discreteness of digital computers is a detail, which should not, in this case, receive much emphasis. The numbers used by actual computers form a finite subset of the rationals, which however for most practical computations form a sufficiently dense subset of $\mathbb{R}$ to be a useful approximation of 'real' reals. A useful idealization of actual computers would then be a machine whose basic actions are conditional branches, and evaluation of formulas involving real (or complex) numbers. This is, very briefly, the point of view taken in [BSS89]; see also [Shu94, BCSS96] and the references there. With this in mind, we in this book present algorithms acting on ordinary real numbers, and consider this to be a reasonable idealization of the actual implementation.

6.2 Motivation: Gröbner bases

In this section we develop, without proofs, the notion of Gröbner bases for ideals. In the next section a generalization is given, which is presented along the same

lines. This section will step over many details, with the intention of suggestion a slightly different point of view towards Gröbner bases, rather than to prove the main theorems once more. An attempt at rigor will again be made from section 6.3 onwards.

6.2.1 Term orders for Gröbner bases

An important ingredient for Gröbner bases is the *term order*, an ordering of the monomials. To any polynomial $f \neq 0$, a monomial $\mathsf{LM}\, f$ is associated. It is called the *leading monomial*, and it is the largest monomial occurring in the polynomial, with respect to the term order. The coefficient associated to this monomial is called the *leading coefficient* (a real number, for now), and is denoted by $\mathsf{LC}\, f$. The product of these is the *leading term*: $\mathsf{LT}\, f = \mathsf{LC}(f)\, \mathsf{LM}(f)$.

The term orders that are used in this context, and the associated leading-monomial functions, have the following properties: (f, g, h nonzero polynomials)

a) The term order $\leq$ is a linear (or total) order, i.e., (1) it is transitive, (2) for any pair of monomials m, m' we have $m \leq m'$ or $m' \leq m$, and (3) if both hold then $m = m'$.
b) The term order $\leq$ is a well-order, i.e., every nonempty set of monomials has a smallest element.
c) $\mathsf{LM}\, f \leq \mathsf{LM}\, g \;\Leftrightarrow\; \mathsf{LM}(hf) \leq \mathsf{LM}(hg)$.
d) The set $\{\mathsf{LM}\, f | f \text{ a polynomial}\}$ forms a basis of the polynomial ring.
e) $\mathsf{LM}(f - \mathsf{LT}\, f) < \mathsf{LM}\, f$.
f) $\mathsf{LM}(f - g) \leq \max(\mathsf{LM}\, f, \mathsf{LM}\, g)$, and equality holds unless $\mathsf{LT}\, f = \mathsf{LT}\, g$.

These properties are not independent. Later we shall extend the notion of 'monomial' and 'monomial order', and require only some of the properties above to hold. For convenience later on, we set $\mathsf{LM}\, 0 = \mathsf{LT}\, 0 = 0$, and also $0 < m$, for all monomials m.

Examples For one variable there is only one term-order: $1 < x < x^2 < \cdots$. With more variables it becomes more interesting. The *lexicographic order*, or *lex-order* for short, symbolically $<_{\text{lex}}$, is defined by $x^\alpha <_{\text{lex}} x^\beta$ iff the left-most nonzero entry in $\alpha - \beta \in \mathbb{Z}^n$ is negative;[2] for example $x_1^2 x_2^{10} <_{\text{lex}} x_1^3$, but $x_1^3 x_2^{10} >_{\text{lex}} x_1^3$. This order is an example of an *elimination order* (for x_n): A Gröbner basis of an ideal with respect to this term order contains a polynomial from which the variables $x_1, \ldots, x_{n-1}$ are eliminated, if the ideal contains such elements at all.

A direct Gröbner basis calculation using the lexicographic order can take much time. *Graded* term orders perform much better. This is especially true for the *graded reverse lexicographic order*, or *grevlex* for friends. It is defined by $x^\alpha <_{\text{grevlex}} x^\beta$ iff $\deg(x^\alpha) < \deg(x^\beta)$, or $\deg(x^\alpha) = \deg(x^\beta)$ and the right-most nonzero entry in $\alpha - \beta$ is positive. (Here $\deg(x^\alpha) = \alpha_1 + \cdots + \alpha_n$.)

[2] Here we use the multi-index notation $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$.

There exist $n!$ variants of the lex- and grevlex-orders, obtained by permuting the variables. Many more term orders satisfying the properties (a) to (f) above exist, and a full classification is given in appendix A.1.

6.2.2 Basic question

The defining property of a Gröbner basis can be expressed using the leading-monomial function LM. Let h_i be some polynomials, and let $I = \langle h_i \rangle$ be the associated ideal. Let $\mathsf{LM}\, I := \mathrm{span}_{\mathbb{R}}\{\mathsf{LM}\, f | f \in I\}$ be the linear span of all leading monomials of ideal members. The set $\mathsf{LM}\, I$ is in general difficult to describe. On the other hand, the ideal $\langle \mathsf{LM}\, h_1, \ldots, \mathsf{LM}\, h_k \rangle$ is a monomial ideal with explicit generators. This ideal is easy to work with, for example the membership problem is trivial.

In general $\langle \mathsf{LM}\, h_1, \ldots, \mathsf{LM}\, h_k \rangle \subseteq \mathsf{LM}\, \langle h_1, \ldots, h_k \rangle$. We are interested in the following question: Given a set of generators $\{h_1, \ldots, h_k\}$ of an ideal, under what conditions is it true that

$$\mathsf{LM}\, \langle h_1, \ldots, h_k \rangle = \langle \mathsf{LM}\, h_1, \ldots, \mathsf{LM}\, h_k \rangle \quad ? \tag{6.1}$$

Bases for which equality holds are called Gröbner bases. It is not difficult to prove that Gröbner bases exist for any ideal (of a Noetherian ring, to be precise). A very natural question to ask is: Given a set of generators $\{h_1, \ldots, h_m\}$ for an ideal I, how can one modify this set of generators such that they still generate I but at the same time also satisfy (6.1)? The algorithm accomplishing this is the *Buchberger algorithm*.

6.2.3 Rephrasing the basic question

We now put the basic question (6.1) in a different form. At this point it is convenient to introduce some notation. Let R be the base ring. For Gröbner bases we use $R = \mathbb{R}[x] = \mathbb{R}[x_1, \ldots, x_n]$, the polynomial ring over $\mathbb{R}$ in n variables.

Consider the diagram of Fig. 6.1. In this diagram M is the free module $R^k = \oplus_{i=1}^k R e_i$, and $e_i = (0, \ldots, 1, \ldots, 0)$ denotes the i-th basis vector in R^k. The map Ψ is an R-module homomorphism mapping e_i to h_i, so that the image of Ψ is the ideal $I = \langle h_1, \ldots, h_k \rangle$. The map $\widetilde{\Psi}$ is also an R-module homomorphism, but this one maps e_i to $\mathsf{LT}\, h_i$. By construction, therefore, the image of $\widetilde{\Psi}$ is contained in $\mathsf{LM}\, I = \mathsf{LT}\, I$. The basic question posed in the previous section can now be rephrased as: Under what conditions do we have that

$$\mathrm{Im}\, \widetilde{\Psi} = \mathsf{LM}\, \mathrm{Im}\, \Psi \quad ? \tag{6.2}$$

Note that $\mathsf{LM}\, \mathrm{Im}\, \Psi \neq \mathrm{Im}(\mathsf{LT}\, \Psi)$: The map $\mathsf{LT}\, \Psi$ is not a linear map, and the diagram of Fig. 6.1 never commutes.

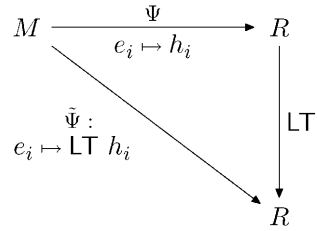

Fig. 6.1 Gröbner basis diagram

6.2.4 A criterion for Gröbner bases

In order to formulate the criterion implying equality in (6.2), we need a few more definitions.

Monomials First of all we extend the notion of *monomial* to M. A monomial in M is an element of the form $x^\beta e_i$ for some $\beta \in \mathbb{N}^n$ and $1 \leq i \leq k$. A *term* is a monomial multiplied by a coefficient.

Standard representations Assume that $\{h_1, \ldots, h_k\}$ is not a Gröbner basis and hence that equality fails in (6.2). In other words, for a certain $\alpha \in M$ we have $\mathsf{LM}\,\Psi\alpha \notin \operatorname{Im}\widetilde{\Psi}$. Consider the set $\{\mathsf{LM}\,\psi t\}$ where t runs over the terms of α. The highest monomial of these is not equal to $\mathsf{LM}\,\Psi\alpha$, as otherwise the latter would be an element of $\operatorname{Im}\widetilde{\Psi}$. In other words, summing all Ψt cancels this highest monomial.

We say that an $\alpha \in M$ is a *standard representation* (of $\Psi\alpha$) if such cancellation of the leading monomial does *not* occur. This can be expressed as: $\mathsf{LM}\,\Psi t \leq \mathsf{LM}\,\Psi\alpha$ for all terms t of α. It is easy to see that every $f \in I = \operatorname{Im}\Psi$ has a standard representation, if and only if $\{h_1, \ldots, h_k\}$ is a Gröbner basis.

Remark 6.1. Our notion of *standard representation* is the natural translation to the current set-up of a similar notion in [BW93, Def. 5.59].

Division; normal form Consider the following algorithm. It is a generalization of the polynomial division algorithm to the case of multiple polynomials. Given an input element f, it expresses f as a member of the ideal $\langle h_1, \ldots, h_k\rangle$ plus a remainder term r, subject to some conditions:

Algorithm 6.2. *(Normal form)*
Input: $f, h_1, \ldots, h_k \in R$
Output: $\alpha \in M,\ r \in R$ *such that*

1. $f = r + \Psi\alpha$
2. $r = 0$ *or* $\mathsf{LM}\,r \notin \operatorname{Im}\widetilde{\Psi}$
3. α *is a standard representation.*

Algorithm:

$\alpha \leftarrow 0$
$r \leftarrow f$
While $r \neq 0$ *and* $\mathsf{LT}\, r = cx^\beta\, \mathsf{LT}(h_i)$ *for some* c, β, i, *do:*
    $\alpha \leftarrow \alpha + cx^\beta e_i$
    $r \leftarrow r - cx^\beta h_i$
EndWhile

Proof: The equality $f = r + \Psi\alpha$ is an invariant of the While-loop: The condition of the While-body implies the second statement, and α is a standard representation because if $\alpha = t_1 + t_2 + \ldots$, where the t_i denote the terms of α in the order in which they were added, then $\mathsf{LM}\,\Psi t_i$, $i = 1, 2, \ldots$ is a strictly decreasing sequence of monomials. Termination, finally, is guaranteed because $\mathsf{LM}\, r$ is strictly decreasing, and the term order is a well-order. ∎

Now if $f \in I$ and $\{h_1, \ldots, h_k\}$ is a Gröbner basis, the algorithm will terminate with $r = 0$ because at each stage $r \in I$ and therefore $\mathsf{LM}\, r \in \operatorname{Im} \widetilde{\Psi} = \langle \mathsf{LM}\, h_1, \ldots, \mathsf{LM}\, h_k \rangle$. In other words, if $\{h_1, \ldots, h_k\}$ is a Gröbner basis the algorithm yields a standard representation for any ideal element. Conversely, if $r = 0$ for any $f \in I$ then $\{h_1, \ldots, h_k\}$ must be a Gröbner basis.

S-polynomials The conclusion of the previous section can be rephrased as: If for any $\alpha \in M$ which is *not* a standard representation, there exists a standard representation β such that $\Psi\alpha = \Psi\beta$, then $\{h_1, \ldots, h_k\}$ is a Gröbner basis.

So how do we find those $\alpha \in M$ which are not standard representations? For such α we have "cancellation of leading monomials". More precisely, let $\alpha = t_1 + t_2 + \cdots$, let $m = \max_i \mathsf{LM}(\Psi t_i) = \widetilde{\Psi} t_p$, and assume the t_i form a non-increasing sequence: $\widetilde{\Psi} t_i = m$ for $i \leq p$, and $\widetilde{\Psi} t_i < m$ for $i > p$. Since α is not a standard representation, $\mathsf{LM}\,\Psi\alpha < m$. As $t_1, \ldots, t_p$ are the only terms involving m this implies $\mathsf{LM}\,\Psi(t_1 + \cdots + t_p) < m$, that is, $\widetilde{\Psi}(t_1 + \cdots + t_p) = 0$. This gives some motivation as to why $\ker \widetilde{\Psi}$ might be of interest. (Note however that α itself need not be an element of $\ker \widetilde{\Psi}$.)

Generators s_{ij} of $\ker \widetilde{\Psi}$ as a module over R are easy to give explicitly:

$$s_{ij} = \frac{\mathsf{LT}\, h_j}{\gcd(\mathsf{LM}\, h_i, \mathsf{LM}\, h_j)} e_i - \frac{\mathsf{LT}\, h_i}{\gcd(\mathsf{LM}\, h_i, \mathsf{LM}\, h_j)} e_j, \qquad (1 \leq i < j \leq k) \tag{6.3}$$

and the images Ψs_{ij} are the well-known S-polynomials, see e.g. [CLO92].

Remark 6.3. *(Binomial kernel)* Note that the s_{ij} are binomials. This is related to the fact that $\widetilde{\Psi}$ is a *monomial mapping*: a mapping that maps monomials to monomials. See also Definition 6.8.

Remark 6.4. *(Buchberger's criteria)* The set of generators (6.3) is not a minimal set. Buchberger's first and second criterion (see e.g. [BW93, CLO92]) may be interpreted as sufficient conditions for generators to be superfluous.

Gröbner bases and Buchberger's algorithm Recall the basic question: Under which condition is $\operatorname{Im}\widetilde{\Psi} = \mathsf{LM}\operatorname{Im}\Psi$. The answer is now easy to give:

Theorem 6.5. *(Gröbner basis) If algorithm 6.2 gives output $r = 0$ on input $f = \Psi(s_{ij})$ for all generators s_{ij} in (6.3), then $\{h_1, \ldots, h_k\}$ is a Gröbner basis.*

Buchberger's algorithm consists of checking the criterion, and adding the nonzero r, which lies in the ideal $\operatorname{Im}\Psi$ by definition of algorithm 6.2, to the ideal generators until the criterion holds. At each step the ideal $\operatorname{Im}\widetilde{\Psi}$ increases. Since the polynomial ring is Noetherian, an increasing chain of ideals stabilizes, implying termination of this algorithm.

6.3 Standard bases

6.3.1 Overview

In this section we put the previous discussion in a more abstract setting. One advantage is that this makes the proof of the Gröbner basis case more transparent. A more important advantage is that it allows for generalizations, in various directions.

One direction is changing the base ring, from the polynomial ring to the ring of formal power series, and later to truncated formal power series. This is of interest to us because formal power series arise naturally from the Birkhoff normal form procedure. Related to the change of base ring is the introduction of non-well-orders for the term orders. The notion of 'leading term' is undefined for formal power series if the term order regards monomials with large exponents as large. The solution is to 'flip' the term order and to regard 1 as the highest monomial. This destroys the well-orderedness however.

A second direction to generalize in is to allow other algebraic structures than ideals, the objects ordinary Gröbner bases deal with. A generalization to modules is well-known, see e.g. [GP88]. Another generalization, for subalgebras, is known as a SAGBI basis [Vas98], or canonical subalgebra basis as Sturmfels [Stu93, Stu96] calls it. For our purposes we need the analogous basis for still different vector spaces. This section gives the basic set-up for all these cases. We formulate the *standard map theorem*, which lies at the heart of all generalizations of Gröbner basis mentioned. In later sections we specialize to several cases of interest.

6.3.2 Definitions

A few details in the definition of term order we use, is different from the usual definition for Gröbner bases; some others, like the Schreyer ordering, need to be generalized. Here we collect the necessary definitions.

Base field The field of coefficients is denoted by $\mathbf{R}$; see also Sect. 6.1.1 for remarks. Note that it is sometimes useful to compute over a coefficient *ring*, see e.g. [AHLM99, Mil96]; we shall not use this.

Term order and monomials Let M be some vector space over $\mathbf{R}$. Already in the previous section we used the name 'monomial' also for elements of the form $x^\beta e_i$, which formed a basis of the free module R^k. Presently we want to be even more general. It is not possible to be very specific about the term 'monomial' here, because we do not want to be specific about the vector space M. For example, for Gröbner bases M is a module, but for canonical subalgebra bases M would be a ring. So instead, we just suppose a set of monomials has been defined, together with a term order. Also we suppose the functions LM and LC, for *leading monomial* and *leading coefficient* are defined on M.

The functions $\mathsf{LM} : M \to M$ and $\mathsf{LC} : M \to \mathbf{R}$ are required to have the following basic properties, for all $f \in M$ and $a \in \mathbf{R}$:

1. $\mathsf{LM}\,\mathsf{LM}\,f = \mathsf{LM}\,f$ (provided $f \neq 0$)
2. $\mathsf{LC}\,\mathsf{LM}\,f = 1$ (provided $f \neq 0$)
3. $\mathsf{LM}\,af = \mathsf{LM}\,f$ (provided $a \neq 0$)
4. $\mathsf{LC}\,af = a\,\mathsf{LC}\,f$

The leading term, denoted by LT, is defined as $\mathsf{LT}\,f = \mathsf{LC}\,f \cdot \mathsf{LM}\,f$. The ordering of the monomials is extended to the terms by simply ignoring the coefficient. (However, if we write $t = t'$ we mean that $t - t' = 0$, instead of just $t \leq t'$ and $t' \leq t$ with respect to the term order.) The other properties we require of the leading-monomial function (and the related term order) are:

a) The set $\mathrm{span}_{\mathbf{R}}\{\mathsf{LM}\,f | f \in M\}$ is dense in M.
b) The term order $\leq$ is a linear (or total) order: For any pair of monomials m, m' we have $m \leq m'$ or $m' \leq m$, and if both hold then $m = m'$, and the term order is transitive.
c) $\mathsf{LM}(f - g) \leq \max(\mathsf{LM}\,f, \mathsf{LM}\,g)$, and equality holds unless $\mathsf{LT}\,f = \mathsf{LT}\,g \neq 0$.

For convenience we also set $\mathsf{LM}\,0 = 0$. A few remarks are in order:

– Generally, M is an infinite dimensional $\mathbf{R}$-vector space.
– Property (c), (1) and (3) together imply that

$$\mathsf{LM}(f - \mathsf{LT}\,f) < \mathsf{LM}\,f, \qquad (f \neq 0) \tag{6.4}$$

– From (4) and (c) it follows that $\mathsf{LT}\,0 = 0$, and $0 < m$ for all (nonzero) monomials m.
– The term order is not required to be a well-order.
– The leading-monomial function is not required to be multiplicative.

In relation to the last remark, note that M need not be a ring, or even a module over some ring, so that it is not clear what 'multiplicative' should mean. This

level of generality is only needed here, and is enough to formulate the main result of this section, the standard map theorem. In the applications of Sect. 6.4 we always require the term order to be multiplicative, in some appropriate sense.

For a linear subspace L of M, we write $\mathsf{LM}\, L$ for the closure of $\operatorname{span}_{\mathbf{R}}\{\mathsf{LM}\, f | f \in L\}$. For example, we have $M = \mathsf{LM}\, M$. Another example, if M is a ring and L an ideal, then $\mathsf{LM}\, L$ is the leading monomial ideal, also called the *initial ideal*.

Refined term orders Suppose we have a (linear) map $\Psi : L \to M$, and term orders on L and M. For clarity we write LM_L and LM_M for the leading-monomial functions on L and M respectively. The term order on L is said to be a *refinement* of the one on M (via Ψ, if we want to be precise), if

$$\mathsf{LM}_M \Psi\alpha \;\leq_M\; \mathsf{LM}_M \Psi \mathsf{LM}_L \alpha \tag{6.5}$$

for all $\alpha \in L$. Using the basic properties, this implies that for all monomials $m, m' \in L$ we have

$$\mathsf{LM}_M\ \Psi m <_M \mathsf{LM}_M\ \Psi m' \quad\Rightarrow\quad m <_L m', \tag{6.6}$$

$$m <_L m' \quad\Rightarrow\quad \mathsf{LM}_M \Psi m \;\leq_M\; \mathsf{LM}_M \Psi m', \tag{6.7}$$

which motivates the name *refinement*. If L is a free module over M, the refined term order on L is called the Schreyer order, see [GP88, Sch91].

Assumption From here on, it will be assumed that whenever there is a map $\Psi : L \to M$ and a term order on M, there is also a term order on L which is a refinement, via Ψ, of the order on M. Moreover we will just write LM instead of LM_L or LM_M; which one is intended will be clear from the context.

Standard representations Using the refined term orders, it is possible to give an elegant definition of a standard representation (see Sect. 6.2.4). Again assume we have a map $\Psi : M \to R$, then an element $\alpha \in M$ is said to be a standard representation if cancellation of leading monomials does not occur:

Definition 6.6. *An element $\alpha \in M$ is called a* standard representation *(of $\Psi\alpha$) if*

$$\mathsf{LM}\, \Psi\alpha = \mathsf{LM}\, \Psi\, \mathsf{LM}\, \alpha.$$

6.3.3 Setup

Now we formulate the analogue of the basic question posed in section 6.2.2 in the current context. Assume we have a linear map $\Psi : M \to R$, and we wish to know its image. In particular, we are interested in the set of leading monomials that occur in the image of Ψ.

Related to Ψ is a map $\widetilde{\Psi}$ (see Fig. 6.2). On monomials $m \in M$ it is defined as $\widetilde{\Psi} m := \mathsf{LT}\, \Psi m$, and it is extended to all of M by linear combinations and closure. $\widetilde{\Psi}$ is a monomial map, and it is easy to describe its range. Moreover

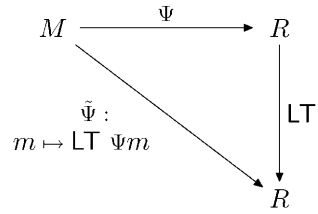

Fig. 6.2 Standard maps and bases

it is clear that $\operatorname{Im}\widetilde{\Psi} \subset \mathsf{LM}\operatorname{Im}\Psi$. The problem is to determine whether in fact $\operatorname{Im}\widetilde{\Psi} = \mathsf{LM}\operatorname{Im}\Psi$. When this is true, Ψ is called a *standard map*. (Usually Ψ is defined in terms of some basis, which is then called a *standard basis*.)

A related problem is to find the kernel of Ψ. In the case where $\operatorname{Im}\Psi$ is the ideal $\langle h_1, \ldots, h_k \rangle$, this is the question of finding the so-called *syzygies* for the ordered set of polynomials $\{h_1, \ldots, h_k\}$, i.e., k-tuples of polynomials $(a_1, \ldots, a_k)$ such that

$$a_1 h_1 + \cdots + a_k h_k = 0.$$

It is easy to see that the set of these k-tuples indeed forms an R-module. The standard map theorem below gives a relation between the kernel of Ψ and the kernel of $\widetilde{\Psi}$, which in the case of ideals boils down to a relation between syzygies of the set $\{h_1, \ldots, h_k\}$ and those of the set $\{\mathsf{LM}\, h_1, \ldots, \mathsf{LM}\, h_k\}$. The latter module is generated by the (pre-images of the) S-polynomials (6.3).

Remark 6.7. *(Syzygies)* Below we shall use the word *syzygy* to refer to syzygies on *leading monomials* of generators, i.e., elements of $\ker\widetilde{\Psi}$ instead of elements of $\ker\Psi$.

6.3.4 Normal form property

In the case of Gröbner bases, that is, a well-order and a polynomial ring, we used algorithm 6.2 to bring an arbitrary element of the polynomial ring into a normal form. The analogue of the algorithm can be written down in the current general context, but will in general not terminate. So instead of writing down a normal form algorithm, we assume existence of a *normal form map* with the necessary properties. The normal form map that we use here is very similar to the one used by Greuel [GP88], with the difference that he does not consider the α–part – see below.

Assume we have the situation of Fig. 6.2. A *normal form map* for $\Psi : M \to R$ is a map

$$\mathrm{NF}^{\Psi} : \quad R \to M \oplus R : \quad f \mapsto \mathrm{NF}^{\Psi}(f) \;=\; \big(\mathrm{NF}^{\Psi}_{\alpha}(f), \mathrm{NF}^{\Psi}_{r}(f)\big)$$

with the following properties (we write $r = \mathrm{NF}^{\Psi}_{r}(f)$, $\alpha = \mathrm{NF}^{\Psi}_{\alpha}(f)$):

a) $f = \Psi\alpha + r$,
b) $r = 0$ or $\mathsf{LM}\, r \notin \operatorname{Im} \widetilde{\Psi}$,
c) α is a standard representation.

Heuristically, the map NF^{Ψ} performs a *division*, with α the 'quotient' and r the 'remainder'. The map Ψ is said to have the *normal form property* if a normal form map NF^{Ψ} exists. This normal form property holds under very general (topological) conditions; for example it always exists in polynomial rings with a well-order as term order.

6.3.5 The standard map theorem

The following theorem is inspired on the proof of the standard basis theorem (for ideals in the local polynomial ring, with non-well-orders) by Greuel [GP88], which he in turn attributes partly to Schreyer [Sch91].

Definition 6.8. *A linear map $\widetilde{\Psi}$ is called a* monomial map *if $\widetilde{\Psi} m$ is a monomial for every monomial m.*

Given a map Ψ, its associated monomial map $\widetilde{\Psi}$ is defined on the set of monomials m by $\widetilde{\Psi} m := \mathsf{LT}\, \Psi m$, and extended linearly for other elements. This is a good definition if $\Psi m \neq 0$ for all monomials m, which will be assumed. Now recall the definition of *standard map*:

Definition 6.9. *Let $\widetilde{\Psi}$ be the monomial map associated to Ψ. The map Ψ is called a* standard map *if*

$$\mathsf{LM} \operatorname{Im} \Psi = \operatorname{Im} \widetilde{\Psi}.$$

Theorem 6.10. *(Standard map theorem) Let L, M, R be vector spaces, and $\Phi : L \to M$ and $\Psi : M \to R$ linear maps, having associated monomial maps $\widetilde{\Phi}$ and $\widetilde{\Psi}$, and assume they have the following properties:*

a) $\operatorname{Im} \Phi \subseteq \ker \Psi$,
b) $\operatorname{Im} \widetilde{\Phi} \supseteq \mathsf{LM} \ker \widetilde{\Psi}$,
c) $\Phi : L \to M$ *has the normal form property.*

Then:

1. $\operatorname{Im} \Phi = \ker \Psi$,
2. $\operatorname{Im} \widetilde{\Psi} = \mathsf{LM} \operatorname{Im} \Psi$,
3. $\operatorname{Im} \widetilde{\Phi} = \mathsf{LM} \operatorname{Im} \Phi$.

In other words, the conclusion of the theorem is that $L \xrightarrow{\Phi} M \xrightarrow{\Psi} R$ is an exact sequence, and Φ and Ψ are standard maps. When applying the theorem, one constructs Φ such that condition (a) is satisfied. Condition (b) is easy to check, as it involves only monomial maps. It corresponds to the Gröbner basis criterion (Theorem 6.5) in the case of polynomial ideals.

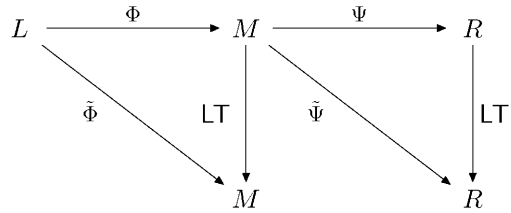

Fig. 6.3 Diagram for the standard map theorem

Proof: Choose any $\beta \in M$, and let $f := \Psi\beta$ be its image in R. Let NF^{Φ} be a normal form for Φ (which exists by assumption (c)), and set $A := \mathrm{NF}^{\Phi}_{\alpha}(\beta)$ and $\rho := \mathrm{NF}^{\Phi}_{r}(\beta)$. Then we have:

$$\beta = \Phi A + \rho, \qquad \rho = 0 \text{ or } \mathsf{LM}\,\rho \notin \operatorname{Im}\widetilde{\Phi}. \tag{6.8}$$

By assumption (a) we have $\Phi A \in \ker\Psi$. Therefore

$$f = \Psi\beta = \Psi(\Phi A + \rho) = \Psi\rho.$$

We now claim: Either $f \neq 0$ and $\mathsf{LM}\,f = \mathsf{LM}\,\Psi\,\mathsf{LM}\,\rho$, or $\rho = 0$. To prove this, assume $\rho \neq 0$ and define

$$\begin{aligned} t_1 &:= \mathsf{LT}\,\rho, \\ \rho' &:= \rho - t_1, \\ t_2 &:= \mathsf{LT}\,\rho'. \end{aligned}$$

Then $\mathsf{LM}\,t_1 > \mathsf{LM}\,t_2 = \mathsf{LM}\,\rho'$, and using (6.5) and (6.7) we get $\mathsf{LM}\,\Psi t_1 \geq \mathsf{LM}\,\Psi t_2 \geq \mathsf{LM}\,\Psi\rho'$. Now if $\mathsf{LM}\,\Psi t_1 > \mathsf{LM}\,\Psi t_2$, then $\mathsf{LM}\,\Psi\rho = \mathsf{LM}(\Psi t_1 + \Psi\rho') = \mathsf{LM}\,\Psi t_1 = \mathsf{LM}\,\Psi\,\mathsf{LM}\,\rho$, proving our claim. So assume on the contrary that $\mathsf{LM}\,\Psi t_1 = \mathsf{LM}\,\Psi t_2$. In particular $\mathsf{LC}\,\Psi t_2 \neq 0$, hence also $\mathsf{LC}\,\widetilde{\Psi} t_2 \neq 0$. Define

$$t_2' := \frac{\mathsf{LC}\,\widetilde{\Psi} t_1}{\mathsf{LC}\,\widetilde{\Psi} t_2} t_2.$$

Then $\widetilde{\Psi} t_1 = \widetilde{\Psi} t_2'$, that is, $t_1 - t_2' \in \ker\widetilde{\Psi}$. Taking the LM on both sides yields $\mathsf{LM}\,t_1 \in \mathsf{LM}\ker\widetilde{\Psi}$. Since $\mathsf{LM}\,t_1 = \mathsf{LM}\,\rho$ and $\mathsf{LM}\ker\widetilde{\Psi} \subseteq \operatorname{Im}\widetilde{\Phi}$ (assumption (b)), this implies $\mathsf{LM}\,\rho \in \operatorname{Im}\widetilde{\Phi}$, contradicting (6.8).

So indeed $f \neq 0$ and $\mathsf{LM}\,f = \mathsf{LM}\,\Psi\,\mathsf{LM}\,\rho = \widetilde{\Psi}\,\mathsf{LM}\,\rho$, or $\rho = 0$. The first part proves that $\mathsf{LM}\operatorname{Im}\Psi \subseteq \operatorname{Im}\bar{\Psi}$. As the other inclusion is trivial, this proves (2). The second part says that if $\beta \in \ker\Psi$ then $\rho = \mathrm{NF}^{\Phi}_{r}(\beta) = 0$, that is, $\beta = \Phi A$. In other words $\ker\Psi \subseteq \operatorname{Im}\Phi$. Together with (a) this proves (1). Finally, using (1) we get that $\mathrm{NF}^{\Phi}_{r}(\beta) = 0$ for all $\beta \in \operatorname{Im}\Phi$, so that every such β has a standard representation, implying (3). ∎

The following two lemmas will be helpful in applying the standard map theorem 6.10.

Binomial lemma In the case of Gröbner bases, the kernel of $\widetilde{\Psi}$ is generated by binomials, which correspond to the S-polynomials. This holds more generally. The following lemma is a generalization of Lemma 4.1 of [Stu96]. The proof is different, since we cannot use the well-ordering property of the term order. (Recall that a *term* is a monomial multiplied by a constant.)

Lemma 6.11. *(Binomial generators) Let $\widetilde{\Psi}$ be a monomial map. Then* $\ker \widetilde{\Psi}$ *is the closure of*

$$\operatorname{span}_{\mathbf{R}}\{t - t' | t, t' \text{ terms, and } \widetilde{\Psi}t = \widetilde{\Psi}t'\}. \tag{6.9}$$

Proof: First define $\widehat{R} := \{\mathsf{LM}\, f | f \in R\}$, and $\widehat{M} := \{\mathsf{LM}\, f | f \in M\}$. For every $r \in \widehat{R}$ select an $m_r \in \widehat{M}$ such that $\widetilde{\Psi}m_r = c \cdot r$ (if one exists), for some $c \in \mathbf{R}$. Now let $\alpha \in \ker \widetilde{\Psi}$. Using that M is the closure of $\operatorname{span}_{\mathbf{R}} M$, we may write $\alpha = \sum_{m \in \widehat{M}} c_m m$. Define

$$\alpha' := \sum_{m \in \widehat{M}} \left(c_m m - c_m \frac{\mathsf{LC}\, \widetilde{\Psi}m}{\mathsf{LC}\, \widetilde{\Psi}m_{\mathsf{LM}\, \widetilde{\Psi}m}} m_{\mathsf{LM}\, \widetilde{\Psi}m} \right).$$

Write $r = \mathsf{LM}\, \widetilde{\Psi}m$, then

$$\widetilde{\Psi}\left(c_m \frac{\mathsf{LC}\, \widetilde{\Psi}m}{\mathsf{LC}\, \widetilde{\Psi}m_r} m_r \right) = c_m \frac{\mathsf{LC}\, \widetilde{\Psi}m}{\mathsf{LC}\, \widetilde{\Psi}m_r}\, \mathsf{LC}(\widetilde{\Psi}m_r)\, \mathsf{LM}(\widetilde{\Psi}m_r) = c_m \mathsf{LC}(\widetilde{\Psi}m) r = \widetilde{\Psi}(c_m m),$$

since $\mathsf{LM}\, \widetilde{\Psi}m_r = r$. This shows that α' is in the closure of (6.9). For any $r \in \widehat{R}$, the sum of the coefficients $c_m\, \mathsf{LC}\, \widetilde{\Psi}m$ over all m such that $m_{\mathsf{LM}\, \widetilde{\Psi}m} = m_r$ vanishes, since this is precisely the coefficient of r in $\widetilde{\Psi}\alpha$. But this means that $\alpha' = \alpha$, which completes the proof. ∎

Standard representations of syzygies The following lemma asserts that syzygies cannot be standard representations:

Lemma 6.12. *Let $t_1 - t_2$ be a binomial in the kernel of $\widetilde{\Psi}$, and let α be a standard representation of $\Psi(t_1 - t_2)$. Then $t_1 > \mathsf{LM}\, \alpha$.*

Proof: Since $t_1 - t_2 \in \ker \widetilde{\Psi}$ we have $\mathsf{LT}\, \Psi t_1 = \mathsf{LT}\, \Psi t_2$. By (6.4) it follows that $\mathsf{LM}\, \Psi t_1 > \mathsf{LM}\, \Psi(t_1 - t_2) = \mathsf{LM}\, \Psi\alpha = \mathsf{LM}\, \Psi\, \mathsf{LM}\, \alpha$, the last equality holding since α is a standard representation. By (6.6), this implies $t_1 > \mathsf{LM}\, \alpha$. ∎

6.3.6 Normal form algorithm

It often happens that a map Ψ not only has the normal form property (see Sect. 6.3.4), but there even exists an algorithm that computes this normal form. Often this algorithm is the following. Note that when h_i are polynomials and Ψ is the module homomorphism $(f_1, \ldots, f_r) \mapsto \sum_i h_i f_i$ into the polynomial ring, then the algorithm below is just algorithm 6.2.

Algorithm 6.13. *(Normal form)*
Input: *Map* $\Psi : M \to R$ *and associated monomial map* $\widetilde{\Psi}$.
Output: $\alpha \in M,\ r \in R$ *such that*

1. $f = r + \Psi\alpha$,
2. $r = 0$ *or* $\mathsf{LM}\, r \notin \operatorname{Im} \widetilde{\Psi}$,
3. α *is a standard representation.*

Algorithm:

$\alpha \leftarrow 0$
$r \leftarrow f$
While $\mathsf{LT}\, r \in \operatorname{Im} \widetilde{\Psi}$, *say* $\mathsf{LT}\, r = \widetilde{\Psi} t$, t *a term, do:*
    $\alpha \leftarrow \alpha + t$,
    $r \leftarrow r - \Psi t$
EndWhile

In general it may be nontrivial to decide whether a term $\mathsf{LT}\, r$ is in the image of $\widetilde{\Psi}$ or not, and to find a term t in the pre-image.

Correctness of algorithm 6.13 is straightforward, but termination less so. If algorithm 6.13 does not terminate, there may exist other algorithms that do. One example is Mora's normal form for the rational function ring; see [GP88, Mor82, Mor85].

6.3.7 Reduced normal forms

For computations it is sometimes useful to use a more restricted notion of normal form, the *reduced normal form*. Indeed, the algorithm of this section will find application in Chap. 7. Whereas the 'remainder' $r = \mathrm{NF}_r^{\Psi}$ of an ordinary normal form need only satisfy $\mathsf{LM}\, r \notin \operatorname{Im} \widetilde{\Psi}$, for a reduced normal form this is required, not only of the leading monomial, but of *all* terms of r. In practice this means that computing such reduced normal forms is less efficient compared to ordinary normal forms. The big asset of reduced normal forms is that the r-part of their output is *unique*, when computed relative to a standard basis.

It is not true that the normal form property also implies the existence of a *reduced* normal form: in the rational function ring the Mora normal form exists, which cannot be extended to a reduced normal form. However, in many cases a reduced normal form does exist, and the algorithm below usually suffices:

Algorithm 6.14. *(Reduced normal form)*
Input: *Map* $\Psi : M \to R$ *and associated monomial map* $\widetilde{\Psi}$.
Output: $\alpha \in M,\ r \in R$ *such that*

1. $f = r + \Psi\alpha$
2. $r = \sum_{i \in I} t_i$ *with* t_i *terms such that* $t_i \notin \operatorname{Im} \widetilde{\Psi}$
3. α *is a standard representation.*

Algorithm:

$\alpha \leftarrow 0$
$r \leftarrow 0$
$g \leftarrow f$
While $g \neq 0$ *do the following:*
    If $\mathsf{LT}\, g \in \operatorname{Im} \widetilde{\Psi}$, *say* $\mathsf{LT}\, g = \widetilde{\Psi} t$, t *a term, then:*
        $\alpha \leftarrow \alpha + t$,
        $g \leftarrow g - \Psi t$
    Else:
        $r \leftarrow r + \mathsf{LT}\, g$
        $g \leftarrow g - \mathsf{LT}\, g$
    EndIf
EndWhile

6.4 Instances of standard bases

In this section we apply the previous theory to some known cases, such as Gröbner bases and canonical subalgebra bases. This shows how the current approach unifies some other approaches. The standard map theorem is also used to define the concept of standard basis for a left-right tangent space.

6.4.1 Gröbner bases

Let $\{h_1, \ldots, h_k\}$ be a set of polynomials in $R := \mathbf{R}[x_1, \ldots, x_n] = \mathbf{R}[x]$. Let M be the free R-module $R^k := \oplus_{i=1}^k R e_i$. The R-module homomorphism $\Psi : M \to R$ is defined by $\Psi e_i = h_i$, so that $\operatorname{Im} \Psi = \langle h_1, \ldots, h_k \rangle$. See Fig. 6.1.

For monomials in R we take the ordinary monomials, and in R^k we take the elements of the form $e_i x^\beta$, where e_i is the i-th canonical basis vector. For the term order (on M and R, with the one on M being a refinement via Ψ of term order on R) we take a general well-order, but one which is multiplicative over R, that is, $m < m'$ implies $\widetilde{m}m < \widetilde{m}m'$ for all monomials $m, m', \widetilde{m}$. Then the map $\widetilde{\Psi}$, defined in the general way by $\widetilde{\Psi} m := \mathsf{LT}\, \Psi m$ for monomials $m \in M$, is in fact an R-module homomorphism.

Algorithm 6.2 implements a normal form NF^Ψ on R, so that the normal form property holds in this setting.

Lemma 6.15. $\ker \widetilde{\Psi}$ *is generated, as an* R*-module, by the syzygies*

$$s_{ij} := \frac{\mathsf{LT}(h_j)}{\gcd(\mathsf{LM}\, h_i, \mathsf{LM}\, h_j)} e_i - \frac{\mathsf{LT}(h_i)}{\gcd(\mathsf{LM}\, h_i, \mathsf{LM}\, h_j)} e_j. \qquad (i, j = 1 \ldots m) \tag{6.10}$$

Moreover,

$$\mathsf{LM}\, \langle s_{ij} \rangle = \langle \mathsf{LM}\, s_{ij} \rangle.$$

Proof: By Lemma 6.11, $\ker \widetilde{\Psi}$ is generated, as an $\mathbf{R}$-vector space, by binomials. Let $b := ax^\beta e_i - bx^\delta e_j$ be a binomial in $\ker \widetilde{\Psi}$. Then $ax^\beta \operatorname{LT} h_i = bx^\gamma \operatorname{LT} h_j$. This implies that b is a monomial multiple of s_{ij}; indeed, $b = (ax^\beta \gcd(\operatorname{LM} h_i, \operatorname{LM} h_j)/\operatorname{LT} h_j)s_{ij}$, proving the first claim. For the second claim, let $m \in \operatorname{LM} \ker \widetilde{\Psi}$, then $m = \operatorname{LM} b$ for some binomial $b \in \ker \widetilde{\Psi}$. By the same argument as before, m is a monomial multiple of some $\operatorname{LM} s_{ij}$. ∎

Now we can formulate the result of this section. Recall that $\{h_1, \ldots, h_k\}$ is called a Gröbner basis if $\operatorname{LM} \langle h_1, \ldots, h_k \rangle = \langle \operatorname{LM} h_1, \ldots, \operatorname{LM} h_k \rangle$. (For the definition of standard submodule basis, see Sect. 6.4.2.)

Theorem 6.16. *Let s_{ij} be generators (6.10) of $\ker \widetilde{\Psi}$ as an R-module, and let NF^Ψ be a normal form, and assume that*

$$\mathrm{NF}_r^\Psi(\Psi s_{ij}) = 0 \qquad \text{for all } s_{ij}.$$

Then:

a) $\{h_1, \ldots, h_k\}$ is a Gröbner basis for $\langle h_1, \ldots, h_k \rangle$.
b) $\{s_{ij} - \mathrm{NF}_\alpha^\Psi(\Psi s_{ij}) | 1 \le i < j \le k\}$ is a standard submodule basis for $\ker \Psi$.

Proof: Write $\alpha_{ij} = \mathrm{NF}_\alpha^\Psi(\Psi s_{ij})$, and define $u_{ij} := s_{ij} - \alpha_{ij}$. Let L be the free R-module generated by vectors v_{ij}, and define $\Phi : L \to M$ by $\Phi v_{ij} = u_{ij}$. Since $\mathrm{NF}_r^\Psi(\Psi s_{ij}) = 0$ we have $\Psi s_{ij} = \Psi \alpha_{ij}$, that is $\Psi u_{ij} = 0$. This shows that $\operatorname{Im} \Phi \subseteq \ker \Psi$.

The binomial s_{ij} lies in $\ker \widetilde{\Psi}$, and α_{ij} is a standard representation of Ψs_{ij}, hence by Lemma 6.12 it follows that $\operatorname{LM} s_{ij} > \operatorname{LM} \alpha_{ij}$, in other words $\operatorname{LM} s_{ij} = \operatorname{LM} u_{ij}$. Since $\langle s_{ij} \rangle_{1 \le i < j \le k} = \ker \widetilde{\Psi}$, this shows that $\operatorname{Im} \widetilde{\Phi} = \langle \operatorname{LM} s_{ij} \rangle_{1 \le i < j \le k} = \operatorname{LM}(\langle s_{ij} \rangle_{1 \le i < j \le k}) = \operatorname{LM} \ker \widetilde{\Psi}$, the middle equality holding because of Lemma 6.15.

Finally, the map Φ has the normal form property, because the term orders involved are well-orders. The standard map theorem now applies. The statement $\operatorname{Im} \Phi = \ker \Psi$ means that the u_{ij} generate $\ker \Psi$. The statement that $\operatorname{Im} \widetilde{\Psi} = \operatorname{LM} \operatorname{Im} \Psi$ means that $\{h_1, \ldots, h_k\}$ is a Gröbner basis. Finally, $\operatorname{Im} \widetilde{\Phi} = \operatorname{LM} \operatorname{Im} \Phi$ implies that the u_{ij} form a standard submodule basis (relative to the induced order). This completes the proof. ∎

Buchberger's algorithm Most of the work has now been done. The final keystone is Buchberger's algorithm, which actually computes a Gröbner basis for arbitrary ideals.

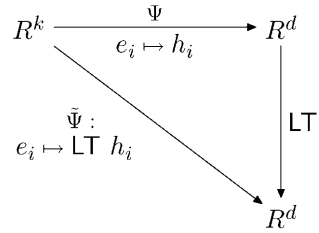

Fig. 6.4 Standard submodule basis diagram

Algorithm 6.17. *(Buchberger's algorithm)*
Input: $\{h_1, \ldots, h_p\} \subset \mathbf{R}[x]$
Output: *A Gröbner basis* $\{h_1, \ldots, h_k\} \subset \mathbf{R}[x]$ *for* $\langle h_1, \ldots, h_p \rangle$.
Algorithm:

$k \leftarrow p$
While $\mathrm{NF}_r^{\Psi}(s_{ij}) \neq 0$ *for any* $1 \leq i < j \leq k$, *do:*
  $h_{k+1} \leftarrow \mathrm{NF}_r^{\Psi}(s_{ij})$
  $k \leftarrow k + 1$
EndWhile

During execution, Ψ is supposed to be defined on $\oplus_{i=1}^{k} \mathbf{R}[x]e_i$, mapping e_i to h_i as usual, for the current value of k.
Proof of Algorithm 6.17: Since $s_{ij} \in \langle h_1, \ldots, h_k \rangle$ implies $\mathrm{NF}_r^{\Psi}(s_{ij}) \in \langle h_1, \ldots, h_k \rangle$, it follows by induction that $h_i \in \langle h_1, \ldots, h_n \rangle$ for any $i > n$. However the ideal $\langle \mathsf{LM}\, h_1, \ldots, \mathsf{LM}\, h_k \rangle$ does increase at each step, implying termination by Hilbert's basissatz. In turn, by Theorem 6.16 this implies that $\{h_1, \ldots, h_k\}$ is a Gröbner basis. ∎

6.4.2 Standard bases for submodules

A straightforward generalization of Gröbner bases gives a useful result for submodules. Gröbner bases are in fact a special case of standard submodule bases; see [GP88].

Let $\{h_1, \ldots, h_k\}$ be elements of $R^d := \oplus_{i=1}^{d} R\epsilon_i$. Here ϵ_i is the i-th basis vector of R^d, and R is the polynomial ring $\mathbf{R}[x_1, \ldots, x_n]$. Let M be the module $R^k := \oplus_{i=1}^{k} Re_i$, where the e_i denote the basis vectors of R^k. The R-module homomorphism $\Psi : M \to R^d$ is defined by $\Psi e_i = h_i$, so that $\mathrm{Im}\, \Psi = \langle h_1, \ldots, h_k \rangle_R$. See figure 6.4.

For monomials in R^d we take the elements of the form $x^{\alpha}\epsilon_i$, as usual, and $x^{\alpha}e_i$ in R^k. Also for the term order on R^d we take an arbitrary multiplicative well-order, and a refinement of it, via Ψ, on R^k. The generic algorithm 6.13 terminates for this setting, implementing a normal form map NF^{Ψ}.

Lemma 6.18. *Write* $\mathsf{LT}(h_i) = x^{\alpha_i} e_{n_i}$. *Then* $\ker \widetilde{\Psi}$ *is generated, as an* R*-module, by the syzygies*

$$s_{ij} = \frac{x^{\gamma_{ij}-\alpha_i}}{\mathsf{LC}\, h_i} e_{n_i} - \frac{x^{\gamma_{ij}-\alpha_j}}{\mathsf{LC}\, h_j} e_{n_j}, \tag{6.11}$$

where the indices i, j *run over the pairs with* $1 \le i < j \le k$ *and* $n_i = n_j$, *and* γ_{ij} *is the exponent of* $\operatorname{lcm}(x^{\alpha_i}, x^{\alpha_j})$. *Moreover,*

$$\mathsf{LM}\,\langle s_{ij}\rangle = \langle \mathsf{LM}\, s_{ij}\rangle,$$

where the indices i, j *run over the same values as in (6.11).*

Proof: The proof is a minor modification of the proof of Lemma 6.15. ∎

A basis $\{h_1, \ldots, h_k\}$ is called a *standard submodule-basis* for $\langle h_1, \ldots, h_k\rangle$ if $\langle \mathsf{LM}\, h_1, \ldots, \mathsf{LM}\, h_k\rangle = \mathsf{LM}\,\langle h_1, \ldots, h_k\rangle$. In terms of the map Ψ this means $\operatorname{Im}\widetilde{\Psi} = \mathsf{LM}\operatorname{Im}\Psi$. The result of this section is the following:

Theorem 6.19. *Let* s_{ij} *be the generators (6.11) of* $\ker\widetilde{\Psi}$ *as an* R*-module, and let* NF^{Ψ} *be a normal form, and assume that*

$$\mathrm{NF}^{\Psi}_r(\Psi s_{ij}) = 0 \qquad \text{for all } s_{ij}.$$

Then:

a) $\{h_1, \ldots, h_k\}$ *is a standard submodule basis for* $\langle h_1, \ldots, h_k\rangle$.
b) $\{s_{ij} - \mathrm{NF}^{\Psi}_{\alpha}(\Psi s_{ij})\}$, *where* ij *runs over the same pairs as in (6.11), is a standard submodule basis for* $\ker\Psi$.

Proof: The proof is word for word the same as that of Theorem 6.16, except that instead of invoking Lemma 6.15, one has to invoke Lemma 6.18. ∎

6.4.3 Standard bases for subalgebras

The bases we consider in this section are known as SAGBI bases (Subalgebra Analogue of Gröbner Bases for Ideals), see e.g. [Vas98]. Sturmfels calls them Canonical Subalgebra bases, see [Stu96, Ch. 11]. We call them 'standard subalgebra bases' to emphasize the similarity with the other cases.

The standard subalgebra basis criterion Let $\{g_1, \ldots, g_m\}$ be polynomials in $R = \mathbf{R}[x]$. Let $M := \mathbf{R}[y_1, \ldots, y_m]$ be the polynomial ring in m variables, and define the ring homomorphism $\Psi : y^{\alpha} \mapsto g_1^{\alpha_1} \cdots g_m^{\alpha_m}$. Then the image of Ψ is the subalgebra of R generated by $g_1, \ldots, g_m$, which we denote by $\mathbf{R}[g_1, \ldots, g_m]$.

In M and R we take the ordinary monomials, and as term order we take any multiplicative well-order, just as in the Gröbner basis case. With such a term order the monomial map Ψ is a ring homomorphism as well. Now we can define what a standard subalgebra basis is:

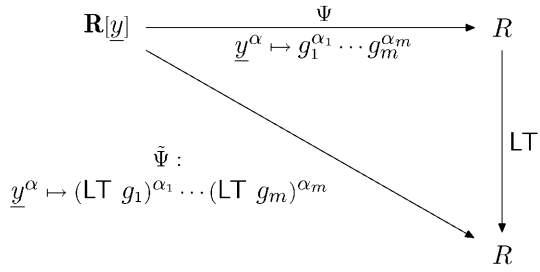

Fig. 6.5 Diagram for standard subalgebra bases

Definition 6.20. *The set* $\{g_1, \ldots, g_m\}$ *is called a* standard subalgebra basis *for the subalgebra* $\operatorname{Im} \Psi = \mathbf{R}[g_1, \ldots, g_m]$ *if* Ψ *is a standard map.*

Note that this is equivalent to: $\mathsf{LM}\, \mathbf{R}[g_1, \ldots, g_m] = \mathbf{R}[\mathsf{LM}\, g_1, \ldots, \mathsf{LM}\, g_m]$.

The criterion for standard subalgebra bases will be formulated in terms of a normal form map for Ψ. To apply this criterion we need an algorithm implementing the normal form. Algorithm6.13 implements such a normal form map NF^Ψ. Termination is guaranteed because $\mathsf{LM}\, r$ is strictly decreasing, and the term order is supposed to be a well-order. It is not yet a proper algorithm, since it is not explained how to decide whether a monomial is in $\operatorname{Im} \widetilde{\Psi}$ or not – but see below.

In order to prove the criterion in Theorem 6.23 below, we need two lemmas:

Lemma 6.21. *The kernel* $\ker \widetilde{\Psi}$ *is an ideal generated by binomials.*

Proof: $\ker \widetilde{\Psi}$ is an ideal since $\widetilde{\Psi}$ is a ring homomorphism, and it is generated as an $\mathbf{R}$-vector space by binomials by Lemma 6.11. A finite number of these binomials therefore generate $\ker \widetilde{\Psi}$ as an ideal. ∎

An element $\alpha \in M$ is called *homogeneous* if it is a sum of terms, each of which is mapped to the same monomial under $\widetilde{\Psi}$. By the previous lemma, $\ker \widetilde{\Psi}$ is generated by homogeneous elements. This notion is used in the following lemma, that is used to relax the condition on the generators of $\ker \widetilde{\Psi}$ in Theorem 6.23 below.

Lemma 6.22. *Let* $s_1, \ldots, s_p$ *be homogeneous generators of* $\ker \widetilde{\Psi}$ *as an ideal. Assume that* $\mathrm{NF}_r^\Psi(\Psi s_i) = 0$ *for all* $i = 1, \ldots, p$. *Then there exists a Gröbner basis* $\{s_i'\}_{i=1}^q$ *of* $\ker \widetilde{\Psi}$ *and representations* $\alpha_1', \ldots, \alpha_q'$ *with the properties (for all* $i = 1, \ldots, q$*):*

$$\left\{ \begin{array}{l} \text{All } s_i' \text{ are homogeneous,} \\ s_i' - \alpha_i' \in \langle s_j - \mathrm{NF}_\alpha^\Psi(\Psi s_j) \rangle_{j=1}^p, \\ \Psi \alpha_i' = \Psi s_i', \\ \widetilde{\Psi}\, \mathsf{LM}\, \alpha_i < \widetilde{\Psi}\, \mathsf{LM}\, s_i'. \end{array} \right. \tag{6.12}$$

Proof: The proof is by induction. First set $s'_i := s_i$ and $\alpha'_i := \mathrm{NF}^{\Psi}_{\alpha}(\Psi s_i)$, then properties (6.12) are satisfied. We turn $\{s'_i\}$ into a Gröbner basis by adding elements that increase $\langle \mathsf{LM}\, s'_i\rangle$, but leave (6.12) invariant.

Assume $\{s'_1, \ldots, s'_q\}$ is not yet a Gröbner basis. Choose an $s \in \ker \widetilde{\Psi}$ such that $\mathsf{LM}\, s \notin \langle \mathsf{LM}\, s'_1, \ldots, \mathsf{LM}\, s'_q\rangle$. Let $m := \widetilde{\Psi}\, \mathsf{LM}\, s$ and write $s = s_{=m} + s_{<m}$ where $s_{=m}$ is the homogeneous leading part of s, and $\widetilde{\Psi}\, \mathsf{LM}\, s_{<m} < m$. Now $\widetilde{\Psi} s_{=m}$ is just m times the coefficient of m in $\widetilde{\Psi} s$, which is zero, so $s_{=m} \in \ker \widetilde{\Psi}$ as well. Since $\ker \widetilde{\Psi} = \langle s'_1, \ldots, s'_q\rangle$ we can write

$$s_{=m} = \sum_{i=1}^{q} a_i s'_i. \qquad (a_i \in R)$$

Since $s_{=m}$ and the s'_i are homogeneous, we may assume that the a_i are homogeneous too. Now

$$\begin{aligned}
\widetilde{\Psi}\, \mathsf{LM}\, s_{=m} &= && \text{(definition)}\\
m &= && \text{(homogeneity)}\\
\widetilde{\Psi} \max_i \mathsf{LM}(a_i s'_i) &= && \text{(compatible term orders)}\\
\max_i \mathsf{LM}(a_i) \widetilde{\Psi}\, \mathsf{LM}\, s'_i &> && \text{(hypothesis)}
\end{aligned}$$

$$\begin{aligned}
\max_i \mathsf{LM}(a_i) \widetilde{\Psi}\, \mathsf{LM}\, \alpha'_i &= && \text{(compatible term orders)}\\
\max_i \widetilde{\Psi}\, \mathsf{LM}(a_i s'_i) &\geq && \text{(property of } \mathsf{LM})\\
\widetilde{\Psi}\, \mathsf{LM} \left(\sum_i a_i s'_i \right). &&&
\end{aligned}$$

So adding $s'_{q+1} := \sum_{i=1}^{q} a_i s'_i$ and $\alpha'_{q+1} := \sum_{i=1}^{q} a_i \alpha'_i$ to the generators and representations, leaves (6.12) invariant while $\langle \mathsf{LM}\, s'_i\rangle_{i=1}^{q+1} \supsetneq \langle \mathsf{LM}\, s'_i\rangle_{i=1}^{q}$. This proves the induction step. Since the ideal $\langle \mathsf{LM}\, s'_i\rangle_{i=1}^{q}$ cannot increase indefinitely, after a finite number of steps $\{s'_1, \ldots, s'_q\}$ is a Gröbner basis. ∎

The following theorem gives a criterion for standard subalgebra bases. It is the analogue of Theorem 6.16, which gives a criterion to recognize Gröbner bases: the S-polynomials should reduce to zero. In this case, the part of the S-polynomials is played by the binomial generators of the so-called toric ideal $\ker \widetilde{\Psi}$ (see e.g. [Stu96]).

Theorem 6.23. *Let $\{s_i\}_{i=1}^{p}$ be generators of $\ker \widetilde{\Psi}$ as an ideal, let NF^{Ψ} be a normal form, and assume that*

$$\mathrm{NF}^{\Psi}_{r}(\Psi s_i) = 0 \qquad \text{for } i = 1, \ldots, p.$$

Then:

a) $\{g_1, \ldots, g_m\}$ *is a standard basis for the subalgebra* $\mathbf{R}[g_1, \ldots, g_m]$.
b) $\{s_i - \mathrm{NF}_\alpha^\Psi(\Psi s_i)\}_{i=1}^p$ *generates* $\ker \Psi$.

Moreover, if $\{s_i\}_{i=1}^p$ *is a Gröbner basis for* $\ker \widetilde{\Psi}$, *then* $\{s_i - \mathrm{NF}_\alpha^\Psi(\Psi s_i)\}_{i=1}^p$ *is a Gröbner basis for* $\ker \Psi$.

Proof: If $\{s_i\}_{i=1}^p$ is a Gröbner basis, set $q = p$ and define $u_i := s_i - \mathrm{NF}_\alpha^\Psi(\Psi s_i)$, $i = 1, \ldots, q$. Since $s_i \in \ker \widetilde{\Psi}$, and $\mathrm{NF}_\alpha^\Psi(\Psi s_i)$ is a standard representation, it follows by Lemma 6.12 that $\mathsf{LM}\, u_i = \mathsf{LM}\, s_i$, and thus $\langle \mathsf{LM}\, u_i \rangle_{i=1}^q = \langle \mathsf{LM}\, s_i \rangle_{i=1}^q = \mathsf{LM} \langle s_i \rangle_{i=1}^q = \mathsf{LM} \ker \widetilde{\Psi}$. Otherwise use Lemma 6.22, and define $u_i := s_i' - \alpha_i'$, $i = 1, \ldots, q$. Then also $\mathsf{LM}\, u_i = \mathsf{LM}\, s_i'$, and $\langle \mathsf{LM}\, u_i \rangle_{i=1}^q = \langle \mathsf{LM}\, s_i' \rangle_{i=1}^q = \mathsf{LM} \langle s_i' \rangle_{i=1}^q = \mathsf{LM} \ker \widetilde{\Psi}$. Note that in both cases we have $u_i \in \langle s_j - \mathrm{NF}_\alpha^\Psi(\Psi s_j) \rangle_{j=1}^p$, for $i = 1, \ldots, q$.

Let L be the free M-module generated by the vectors $e_1, \ldots, e_q$, and define the M-module homomorphism Φ by $\Phi e_i := u_i$. By construction we have $\operatorname{Im} \Phi \subseteq \ker \Psi$, and by the foregoing discussion $\operatorname{Im} \widetilde{\Phi} = \langle \mathsf{LM}\, u_i \rangle_{i=1}^q = \mathsf{LM} \ker \widetilde{\Psi}$.

The map Φ has the normal form property – indeed, algorithm 6.2 provides a normal form – so we may apply the standard map theorem. The first conclusion, $\operatorname{Im} \Phi = \ker \Psi$, proves that $\{u_1, \ldots, u_q\}$ and hence $\{s_i - \mathrm{NF}_\alpha^\Psi(\Psi s_i)\}_{i=1}^p$ generates $\ker \Psi$. The conclusion $\operatorname{Im} \widetilde{\Phi} = \mathsf{LM} \operatorname{Im} \Phi$ implies that the $\{u_1, \ldots, u_q\}$ is a Gröbner basis for $\ker \Psi$. Finally, from $\operatorname{Im} \widetilde{\Psi} = \mathsf{LM} \operatorname{Im} \Psi$ we conclude that $\{g_1, \ldots, g_m\}$ is a standard subalgebra basis for $\mathbf{R}[g_1, \ldots, g_m]$. ∎

Implementing the criterion In order to check the standard subalgebra basis criterion, it is necessary to compute NF^Ψ, and also to compute a (Gröbner) basis for the ideal $\ker \widetilde{\Psi}$. These two problems are solved by the following algorithm.

Algorithm 6.24. *(Gröbner basis and normal form for binomial ideals, or: Finding syzygies for subalgebra bases, and representations of algebra elements.)*
Input: *A monomial ring homomorphism* $\widetilde{\Psi} : \mathbf{R}[y] \to \mathbf{R}[x]$, *an element* $m \in \mathbf{R}[x]$.
Output: *Gröbner basis for* $\ker \widetilde{\Psi}$; *a monomial* t *with* $\widetilde{\Psi} t = m$ *if it exists.*
Algorithm:

Introduce an elimination term order with $\{y_i\} < \{x_j\}$.
Compute a Gröbner basis $\mathcal{G}$ *of* $\langle y_1 - \widetilde{\Psi} y_1, \ldots, y_m - \widetilde{\Psi} y_m \rangle_{\mathbf{R}[y,x]}$ *with respect to* $<$.
Output $\mathcal{G} \cap \mathbf{R}[y]$
Let $t \in \mathbf{R}[y, x]$ *be the normal form of* m *with respect to* $\mathcal{G}$.
If $t \in \mathbf{R}[y]$, *output* t, *otherwise output "*$m \notin \operatorname{Im} \widetilde{\Psi}$*".*

See [Stu96, Alg. 4.5] or [AL94, Th. 4.3.13] for a proof. For more efficient algorithms to compute $\mathcal{G}$, see [Stu96, Ch. 12].

Using this, algorithm 6.13 can be implemented. In general, to compute $\mathrm{NF}^\Psi(f)$ one needs several invocations of algorithm 6.24. The slow Gröbner basis computation for $\mathcal{G}$ is only required once, and the normal form algorithm to compute t is much faster.

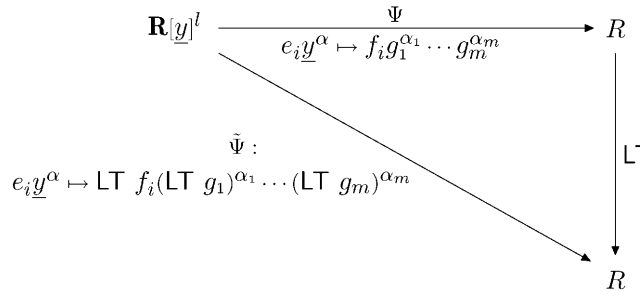

Fig. 6.6 Diagram for bases of modules over subalgebras

The analogue of Buchberger's algorithm If the condition "$\mathrm{NF}_r^{\Psi}(\Psi s_i) = 0$ for all s_i" fails, then adding the nonzero normal forms to the set of generators does not change the subalgebra, but does enlarge the set of monomials in the image of $\widetilde{\Psi}$. The condition can then be checked again, until it holds. This strategy is called the Buchberger algorithm in the case where $\mathrm{Im}\,\Psi$ is an ideal. In that case $\widetilde{\Psi}$ is also an ideal, and because of Hilbert's basissatz these ideals cannot increase indefinitely, assuring termination of the algorithm.

This argument fails in the case of subalgebras, and indeed, it can be shown that (finite) canonical subalgebra bases do not exist for all subalgebras. Perhaps the simplest example is the ideal $\langle x^2 \rangle \subset \mathbf{R}[x]$, considered as an algebra. A basis for this algebra includes polynomials P with $\mathsf{LM}\,P = x^p$, for every prime p. Another example is the ring of polynomials in x_1, x_2, x_3 that are invariant under cyclic permutation of the variables; see [Göb95] or [Stu96, Ch. 11] for details.

6.4.4 Standard bases for modules over subalgebras

As a generalization of the previous section, we now consider modules over subalgebras of polynomial rings. Standard bases for such objects are used in the sequel as building blocks for standard bases for left-right tangent spaces, the ultimate object of our interest.

The standard subalgebra basis criterion Let $\{g_1, \ldots, g_m\}$ and $\{f_1, \ldots, f_l\}$ be polynomials in $R = \mathbf{R}[x]$. The polynomial ring $\mathbf{R}[y_1, \ldots, y_m]$ is again denoted by M. Define the M-module homomorphism $\Psi : M^l \to R : e_i y^\alpha \mapsto f_i g_1^{\alpha_1} \cdots g_m^{\alpha_m}$. See Fig. 6.6; in this figure, e_i is the i-th canonical basis vector of $\mathbf{R}[\underline{y}]^l$. The image of Ψ, which is written as $\{f_1, \ldots, f_l\}\mathbf{R}[g_1, \ldots, g_m]$, is the object of interest. Algorithm 6.13 again implements a normal form. How to compute inverses of $\widetilde{\Psi}$ will be explained below.

The kernel of $\widetilde{\Psi}$ is an M-submodule, generated by binomials. Lemma 6.22 has an obvious counterpart in the current context, with "ideal" replaced by "M-submodule", and "Gröbner basis" by "standard submodule basis". The proof remains valid too.

The following theorem gives a criterion that guarantees Ψ to be a standard map, which, as usual, means that $\mathsf{LM}\,\mathrm{Im}\,\Psi = \mathrm{Im}\,\widetilde{\Psi}$. Here Ψ is defined in terms of two sets of elements, $\{f_i\}$ and $\{g_i\}$. The *pair* $(\{f_i\},\{g_i\})$ is called a *standard basis* for the subalgebra-module $\mathrm{Im}\,\Psi = \{f_i\}\mathbf{R}[g_i]$ if Ψ is a *standard map*. A basis is called a standard subalgebra-module basis if the following criterion is met:

Theorem 6.25. *Let* $\{s_i\}$ *be generators of* $\ker\widetilde{\Psi}$ *as an* M*-submodule, let* NF^{Ψ} *be a normal form, and assume that*

$$\mathrm{NF}^{\Psi}_r(\Psi s_i) = 0 \qquad \textit{for all } s_i.$$

Then:

a) $(\{f_i\},\{g_i\})$ *is a standard basis for the subalgebra-module*

$$\{f_1,\ldots,f_l\}\mathbf{R}[g_1,\ldots,g_m].$$

b) $\{s_i - \mathrm{NF}^{\Psi}_{\alpha}(\Psi s_i)\}$ *generates* $\ker\Psi$.

Moreover, if $\{s_i\}$ *is a standard submodule basis for* $\ker\widetilde{\Psi}$*, then* $\{s_i - \mathrm{NF}^{\Psi}_{\alpha}(\Psi s_i)\}$ *is a standard submodule basis for* $\ker\Psi$.

Proof: The proof is completely analogous to the proof of Theorem 6.23. ∎

Implementing the criterion To turn the above discussion into a computer program, we need an algorithm that compute generators s_i of $\ker\widetilde{\Psi}$ (that is, generators for the syzygies), and an algorithm implementing the normal form map NF^{Ψ}. In the application, the first module generator f_1 is 1, and this fact can be exploited. We specialize to this case. To describe the algorithm we introduce the following notation:

$$\begin{aligned} R_N &= \mathbf{R}[t_2,\ldots,t_l,y_1,\ldots,y_m,x_1,\ldots,x_n],\\ I_N &= \langle t_2 - \mathsf{LM}\,f_2,\ldots,t_l - \mathsf{LM}\,f_l, y_1 - \mathsf{LM}\,g_1,\ldots,y_m - \mathsf{LM}\,g_m\rangle,\\ G_N &= \{g_{N1},\ldots,g_{Nq}\} = \text{Gröbner basis for } I_N \text{ with respect to } \preccurlyeq, \end{aligned}$$

where $\preccurlyeq$ is an elimination term order on R_N with $\{y_i\} \preccurlyeq \{t_i\} \preccurlyeq \{x_i\}$, and which is *graded*, with respect to the total degree, in the variables t_i. Then we have:

Proposition 6.26. *With the definitions above, each binomial in*

$$G_N \cap \{1,t_2,\ldots,t_l\}\mathbf{R}[y_1,\ldots,y_m]$$

is an element of $\ker\widetilde{\Psi}$ *via the binomial correspondence*

$$\begin{aligned} mt_i - m't_j &\mapsto me_i - m'e_j,\\ mt_i - m' &\mapsto me_i - m'e_1,\\ m - m' &\mapsto me_k - m'e_k \quad \textit{for } k = 1,\ldots,l \end{aligned}$$

Here m *and* m' *are arbitrary monomials in* $\mathbf{R}[y]$*. These elements together form a generating set of* $\ker\widetilde{\Psi}$ *as an* $\mathbf{R}[y]$*-module.*

Proof: First note that $I_N \cap \{1, t_2, \ldots, t_l\}\mathbf{R}[y] \subseteq \ker \widetilde{\Psi}$ via the binomial correspondence. For the converse, of the binomials in $\ker \widetilde{\Psi}$ not generated by the elements mentioned above, let α be one with smallest leading monomial. This leading monomial is of the form $t_i m$ or m, with $m \in \mathbf{R}[y]$. Since G_N is a Gröbner basis of I_N, this monomial is a multiple of the leading monomial of some $g \in G_N$. Both terms of g are at most linear in the t_i, and do not involve x_i, by the choice of term order. Subtracting the proper multiple of g from α yields an α' with smaller leading monomial, which by choice of term order again, lies in $G_N \cap \{1, t_2, \ldots, t_l\}$. This provides the required contradiction. ∎

Remark 6.27. *(Efficiency)* It is most efficient to first enlarge the $\{g_i\}$ to a standard subalgebra basis. Then elements $m - m' \in G_N$, each resulting in l syzygies to be checked in the condition of Theorem 6.25, can all be ignored since they will automatically reduce to 0.

Using the Gröbner basis G_N, and the standard map Ψ_N related to it, we can write down a normal form algorithm for Ψ. It is algorithm 6.13 with an explicit subroutine for finding the inverse image of a monomial under $\widetilde{\Psi}$. Here the term order $\preccurlyeq$ is essential.

Algorithm 6.28. *(Normal form for modules over subalgebras)*
Input: *A map* $\Psi : \mathbf{R}[y]^l \to R$ *with* $\Psi e_1 = 1$, *the associated monomial map* $\widetilde{\Psi}$, *a Gröbner basis* G^N *as above, the associated map* $\Psi_N : R_N^q \to R_N$, *and the associated normal form map* NF^{Ψ_N}.
Output: $\alpha \in \mathbf{R}[y]^l$, $r \in R$ *such that*

1. $f = r + \Psi\alpha$,
2. $r = 0$ *or* $\mathsf{LM}\, r \notin \operatorname{Im} \widetilde{\Psi}$,
3. α *is a standard representation.*

Algorithm:

$\alpha \leftarrow 0$
$r \leftarrow f$
BeginLoop
  $m \leftarrow (\mathsf{LT}\, r)$ *with* e_i *replaced by* t_i.
  $r_N \leftarrow \mathrm{NF}_r^{\Psi_N}(m)$
  If $r_N \in \{1, t_2, \ldots, t_l\}\mathbf{R}[y]$, *then*
    If $r_N \in \mathbf{R}[y]$, *then*
      $t \leftarrow e_1 r_N$
    Else
      $t \leftarrow r_N$ *with* t_i *replaced by* e_i
    EndIf
    $\alpha \leftarrow \alpha + t$
    $r \leftarrow r - \Psi t$

Else
ExitLoop
EndIf
EndLoop

Proof: The condition that $\mathsf{LT}\, r \in \operatorname{Im} \widetilde{\Psi}$ is equivalent to the existence of an $r_N \in \{1, t_2, \ldots, t_l\}\mathbf{R}[y]$ that is equal to m modulo I_N. Since the term order favors monomials without x_i's and with lowest-degree t_i's, if such a form exists it is the output of the normal form $\mathrm{NF}_r^{\Psi_N}(m)$. Correctness follows from the invariant $f = r + \Psi\alpha$, and the fact that $\mathsf{LM}\, r$ decreases implies termination, using the well-orderedness of $\preccurlyeq$. ∎

The analogue of Buchberger's algorithm If the basis $(\{f_i\}, \{g_i\})$ defining the map Ψ, is *not* a standard basis, that is $\mathrm{NF}_r^{\Psi}(\Psi s_i) \neq 0$ for some s_i, it may be turned into one by adding elements. There are two possibilities: Either the binomial s_i is of the form $e_j(y^\alpha - y^\beta)$, or it is of the more general form $e_j y^\alpha - e_k y^\beta$ with $j \neq k$. Syzygies of the first form will not occur if $\{g_i\}$ is a standard subalgebra basis to start with (see remark 6.27). Using the normal form of syzygies of the second form, new elements are found and added to the $\{f_i\}$, that increase $\operatorname{Im} \widetilde{\Psi}$ but leave $\operatorname{Im} \Psi$ invariant.

6.4.5 Left-Right tangent space

In Sect. 3.2.3 the codimension of the tangent space to the orbit of a map under left-right transformations was shown to be equal to the codimension of

$$T^r_{\boldsymbol{E}} \;=\; J + \{1, f_1, f_2\}\mathbf{R}[[H, H_2]] \subset R. \tag{6.13}$$

Here R is the ring of formal power series $\mathbf{R}[[\rho_1, \rho_2, \psi, \chi]]$, J is an ideal, and f_1, f_2, H, H_2 are all elements of R. The first problem to solve is: How to compute the codimension of T, and find elements in R complementing it. The second problem is: Given an arbitrary $f \in R$, write it explicitly as a sum of an element of T and a linear combination of the complementing elements. The result of this latter procedure can be used to build explicit reparametrizations connecting an arbitrary deformation to a universal one.

The situation is analogous to the case of unfoldings of functions under right-transformations. There the tangent space was an ideal, the procedure to find the codimension and complementing elements was Buchberger's algorithm (for standard bases), and the normal form procedure computed the required representation for arbitrary functions f, which the algorithm of Kas and Schlessinger used to compute reparametrizations.

The space of equation (6.13) is of the following general form:

$$\langle h_1, \ldots, h_k \rangle + \{f_1, \ldots, f_l\}\mathbf{R}[[g_1, \ldots, g_m]]. \tag{6.14}$$

Spaces of this form are the image of Ψ in Fig. 6.7, except that for simplicity we here use the polynomial ring $R = \mathbf{R}[x]$ as a base ring, instead of the ring of formal

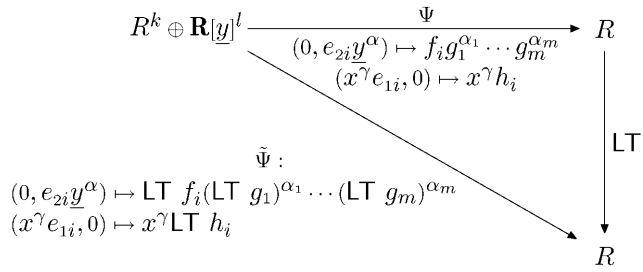

Fig. 6.7 LR-tangent space diagram

power series $\mathbf{R}[[x]]$. In the application we use truncated formal power series, but at this stage this would unnecessarily complicate the notation. Note that the discussion below is independent of the term order; indeed, in the polynomial ring the term order may be, but need not be, a well-order. (However, for a reversed well-order, the reduced normal form does not exist; algorithm 6.14 will not terminate in general.)

In Fig. 6.7, the maps Ψ and $\widetilde{\Psi}$ are defined on elements of the form $(x^\alpha e_{1i}, 0)$ and $(0, e_{2i}y^\alpha)$. By linearity, Ψ is defined on all of on all of $R^k \oplus \mathbf{R}[\underline{y}]^l$. The goal of this section is, first of all, to formulate a condition guaranteeing that $\mathsf{LM}\,\mathrm{Im}\,\Psi = \mathrm{Im}\,\widetilde{\Psi}$. If equality holds, the map Ψ is called a *standard map*, and the triple

$$(\{h_1, \ldots, h_k\}, \{f_1, \ldots, f_l\}, \{g_1, \ldots, g_m\})$$

is called a *standard basis* for the "left-right tangent space" (6.14).

Generators of ker $\widetilde{\Psi}$ In what follows, two natural but different $\mathbf{R}[\underline{y}]$-module structures on $R^k \oplus \mathbf{R}[\underline{y}]^l$ will be used. For lack of better names, we call them the (ordinary) $\mathbf{R}[\underline{y}]$- and monomial $\mathbf{R}[\underline{y}]$-module structures, and multiplication is defined as follows:

$$\begin{aligned} y_i \cdot (a, b) &= (g_i a, y_i b), && \text{(ordinary module structure)} \\ y_i \cdot (a, b) &= (\mathsf{LM}(g_i) a, y_i b). && \text{(monomial module structure)} \end{aligned}$$

By Lemma 6.11 the kernel $\ker \widetilde{\Psi}$ is generated, as a linear vector space, by binomials. Write $\widetilde{\Psi}_1$ for the restriction of $\widetilde{\Psi}$ to $R^k \times \{0\}$, whose image is the ideal $\langle h_i \rangle$, and let $\widetilde{\Psi}_2$ be the restriction of $\widetilde{\Psi}$ to $\{0\} \times \mathbf{R}[\underline{y}]^l$. Then we have the following:

Lemma 6.29. *The kernel of $\widetilde{\Psi}$ is generated, as a linear vector space, by the following three sets of binomials:*

a) $\{(x^\alpha e_{1i} - c x^\beta e_{1j}\ ,\ 0) \in \ker \widetilde{\Psi}_1\}_{1 \le i \le j \le k}$
b) $\{(0\ ,\ y^\alpha e_{2i} - c y^\beta e_{2j}) \in \ker \widetilde{\Psi}_2\}_{1 \le i \le j \le l}$
c) $\{(x^\alpha e_{1i}\ ,\ -c y^\beta e_{2j}) \ \mid\ \widetilde{\Psi}_1(x^\alpha e_{1i}) = \widetilde{\Psi}_2(c y^\beta e_{2j})\}_{1 \le i \le k,\ 1 \le j \le l}$

Moreover, any binomial in the kernel is in one of these three sets.

Proof: By Lemma 6.11, $\ker\widetilde{\Psi}$ is generated by binomials. A binomial in $R^k \oplus \mathbf{R}[\underline{y}]^l$ has both monomials in the first component, both in the second, or exactly one in either, corresponding to the three cases of the lemma. ∎

The binomials of case (a) generate (as vector space) an R-module. It is generated (as an R-module) by the ideal syzygies given in Lemma 6.15. The binomials of case (b) generate (as a vector space) a monomial $\mathbf{R}[y]$-module. Generators of this object are just the subalgebra-module syzygies, which can be computed by algorithm 6.28. It remains to find the binomials of case (c). The linear span of these binomials has a monomial $\mathbf{R}[\underline{y}]$-module structure. The projection of this module onto its second component, $\mathbf{R}[\underline{y}]^l$, is the monomial $\mathbf{R}[\underline{y}]$-module $\widetilde{\Psi}_2^{-1}(\mathsf{LM}\,\langle h_1,\ldots,h_k\rangle)$. This module is generated by monomials. Assuming for the moment that we know its monomial generators $v_i \in \mathbf{R}[\underline{y}]^l$, we can say the following:

Lemma 6.30. *Let $\{s_1,\ldots,s_p\} \subset R^k$ be the ideal syzygies of $\langle h_i\rangle$ as defined in lemma 6.15. Let $\{b_1,\ldots,b_q\} \subset \mathbf{R}[\underline{y}]^l$, be a binomial standard basis of the submodule $\ker\widetilde{\Psi}_2$ (the subalgebra-module syzygies). Let $v_1,\ldots,v_r$ be monomial generators of the submodule $\widetilde{\Psi}_2^{-1}(\mathsf{LM}\,\langle h_1,\ldots,h_k\rangle) \subseteq \mathbf{R}[\underline{y}]^l$. Let $<$ on $R^d \oplus \mathbf{R}[\underline{y}]$ be a refinement of the term-order on R, such that if $m \in \mathbf{R}[\underline{y}]$ and $m' \in R^d$ and $m - m' \in \ker\widetilde{\Psi}$, then $m > m'$. Then, for any $m \in \mathsf{LM}\ker\widetilde{\Psi}$, (at least) one of the following holds:*

a) $m \in \langle \mathsf{LM}\,s_1,\ldots,\mathsf{LM}\,s_p\rangle_R \times \{0\}$,
b) $m \in \{0\} \times \langle \mathsf{LM}\,b_1,\ldots,\mathsf{LM}\,b_q\rangle_{\mathbf{R}[\underline{y}]}$,
c) $m \in \{0\} \times \langle v_1,\ldots,v_r\rangle_{\mathbf{R}[\underline{y}]}$.

Proof: Let $m \in \mathsf{LM}\ker\widetilde{\Psi}$. Then there exists an $m' < m$ such that $m - m' \in \ker\widetilde{\Psi}$. This binomial falls into one of the classes (a), (b) or (c) of Lemma 6.29. In case (a), $m \in \mathsf{LM}\,\langle s_i\rangle \times \{0\} = \langle \mathsf{LM}\,s_i\rangle \times \{0\}$, by Lemma 6.18. In case (b), $m \in \{0\} \times \mathsf{LM}\,\langle b_i\rangle = \{0\} \times \langle \mathsf{LM}\,b_i\rangle$, since $\{b_i\}$ is a standard submodule basis by hypothesis. In case (c) finally, $m \in \{0\} \times \mathbf{R}[\underline{y}]^l$ by the choice of the refined term order. This implies $m' \in \mathsf{LM}\,\langle h_i\rangle \times \{0\}$, hence $m \in \widetilde{\Psi}_2^{-1}\,\mathsf{LM}\,\langle h_i\rangle = \{0\} \times \langle v_i\rangle$. ∎

Now we can describe $\ker\widetilde{\Psi}$ completely:

Lemma 6.31. *Let $\{s_1,\ldots,s_p\}$, $\{b_1,\ldots,b_q\}$ and $\{v_1,\ldots,v_r\}$ be as in Lemma 6.30. Let $w_1,\ldots,w_r \in R^k$ be monomials such that $v_i - w_i \in \ker\widetilde{\Psi}$ for all $1 \le i \le r$. (Here $v_i - w_i$ denotes the element $(-w_i, v_i) \in R^d \oplus \mathbf{R}[\underline{y}]^l$.) Then*

$$\begin{aligned}\ker\widetilde{\Psi} = {} & \langle s_1,\ldots,s_p\rangle_R \times \{0\} \\ & + \{0\} \times \langle b_1,\ldots,b_q\rangle_{\mathbf{R}[\underline{y}]} \\ & + \langle v_1 - w_1,\ldots,v_r - w_r\rangle_{\mathbf{R}[\underline{y}]}\end{aligned} \tag{6.15}$$

where in the last term the monomial $\mathbf{R}[\underline{y}]$-module structure is used.

Proof: By Lemma 6.11 it is enough to check that every *binomial* in $\ker\widetilde{\Psi}$ lies in the right-hand-side of (6.15). So let $m - m'$ be any binomial in $\ker\widetilde{\Psi}$, and suppose $m > m'$. If $m - m'$ is an element of the sets (a) or (b) of Lemma 6.29, then it is an element of $\langle s_i\rangle_R \times \{0\}$ or $\{0\} \times \langle b_i\rangle_{\mathbf{R}[\underline{y}]}$ respectively, since $\{s_i\}$ and $\{b_i\}$ generate the corresponding submodules. If $m-m'$ is in set (c), then by Lemma 6.30(c), $m \in \{0\}\times\langle v_i\rangle_{\mathbf{R}[\underline{y}]}$, say $m = y^\alpha v_i$. Then $(m-m')-y^\alpha(v_i-w_i)$ is in set (b), and these elements are in the right-hand-side of (6.15) as was already shown. ∎

Standard bases for left-right tangent spaces In order to formulate the theorem, we now introduce the map Φ. As in previous cases, the image of Φ will be the kernel of Ψ, if suitable conditions are met. Recall that Ψ_1 is the restriction of Ψ to $R^k \times \{0\}$.

Definition 6.32. *Let $\{s_1,\dots,s_p\}$, $\{b_1,\dots,b_q\}$, $\{v_1-w_1,\dots,v_r-w_r\}$ be as in Lemma 6.31. Let ϵ_{1i} be canonical basis vectors of R^p, let ϵ_{2i} be those of $\mathbf{R}[\underline{y}]^q$ and ϵ_{3i} those of $\mathbf{R}[\underline{y}]^r$. Suppose both Ψ and Ψ_1 have the normal form property, and let NF^{Ψ}, NF^{Ψ_1} be normal forms. Then Φ is defined as follows:*

$$\begin{aligned}
\Phi : R^p \oplus \mathbf{R}[\underline{y}]^q \oplus \mathbf{R}[\underline{y}]^r \to\ & R^k \oplus \mathbf{R}[\underline{y}]^l \\
x^\alpha\epsilon_{1i} \mapsto\ & (x^\alpha s_i, 0) - \left(x^\alpha\,\mathrm{NF}^{\Psi_1}_\alpha(\Psi_1 s_i), 0\right) \quad (i = 1\dots p)\\
y^\beta\epsilon_{2i} \mapsto\ & \left(0, y^\beta b_i\right) - y^\beta\,\mathrm{NF}^{\Psi}_\alpha(\Psi(0,b_i)) \quad (i = 1\dots q)\\
y^\beta\epsilon_{3i} \mapsto\ & y^\beta(v_i-w_i) - y^\beta\,\mathrm{NF}^{\Psi}_\alpha(\Psi(v_i-w_i)) \quad (i = 1\dots r)
\end{aligned}$$

Wherever appropriate, multiplication is according to the ordinary $\mathbf{R}[\underline{y}]$*-module structure.*

The definition of Φ on $R^p \times \{0\} \times \{0\}$ uses the normal form $\mathrm{NF}^{\Psi_1}_\alpha$ instead of $\mathrm{NF}^{\Psi}_\alpha$, since the latter is not guaranteed to map into $R^k \times \{0\}$, and only on that subset can we use the R-module structure, instead of the coarser structure of an $\mathbf{R}[\underline{y}]$-module.

Extending the ordinary $\mathbf{R}[\underline{y}]$-module structure in the obvious way to $R^p \oplus \mathbf{R}[\underline{y}]^q \oplus \mathbf{R}[\underline{y}]^r$, the map Φ becomes an ordinary $\mathbf{R}[\underline{y}]$-module homomorphism. The map $\widetilde{\Psi}$ is defined as usual, by setting $\widetilde{\Psi}m := \mathsf{LM}\,\Psi m$ for monomials, and extending it linearly. Then, similarly extending the *monomial* $\mathbf{R}[\underline{y}]$-module structure to $R^p \oplus \mathbf{R}[\underline{y}]^q \oplus \mathbf{R}[\underline{y}]^r$, makes $\widetilde{\Phi}$ a monomial $\mathbf{R}[\underline{y}]$-module homomorphism.

Theorem 6.33. *Let $\{s_i\} \subset R^k$, $\{b_i\} \subset \mathbf{R}[\underline{y}]^l$ and $\{v_i - w_i\} \subset R^k \oplus \mathbf{R}[\underline{y}]^l$ be as in Lemma 6.31. Let Φ be defined as above. Suppose that*

$$\begin{aligned}
&1.\ \mathrm{NF}^{\Psi_1}_r(\Psi_1 s_i) = 0, && (i = 1\dots p)\\
&2.\ \mathrm{NF}^{\Psi}_r(\Psi(0,b_i)) = 0, && (i = 1\dots q)\\
&3.\ \mathrm{NF}^{\Psi}_r(\Psi(v_i-w_i)) = 0. && (i = 1\dots r)
\end{aligned}$$

Then:

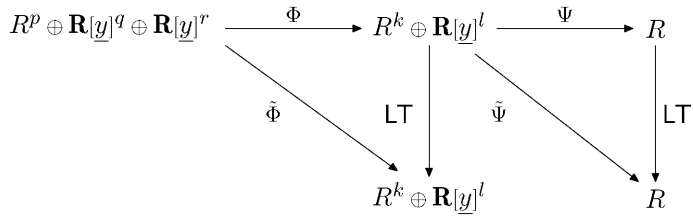

Fig. 6.8 The full LR-tangent space diagram

a) The triple

$$(\{h_1, \ldots, h_k\}, \{f_1, \ldots, f_l\}, \{g_1, \ldots, g_m\})$$

forms a standard basis for

$$\operatorname{Im} \Psi = \langle h_1, \ldots, h_k \rangle_R + \{f_1, \ldots, f_l\}\mathbf{R}[g_1, \ldots, g_m].$$

b) The map Φ is a standard map, and $\operatorname{Im} \Phi = \ker \Psi$.

Proof: Assumptions 1 to 3, together with the definition of Φ as an ordinary $\mathbf{R}[\underline{y}]$-module homomorphism, imply that $\operatorname{Im} \Phi \subseteq \ker \Psi$. By Lemma 6.12 applied to $\bar{\Psi}$ and Ψ_1 and their corresponding normal forms, we find the following:

$$\begin{aligned}
\mathsf{LM}\, \Phi \underline{x}^\alpha \epsilon_{1i} &= \mathsf{LM}(\underline{x}^\alpha s_i, 0) \\
\mathsf{LM}\, \Phi \underline{y}^\beta \epsilon_{2i} &= \mathsf{LM}(0, \underline{y}^\beta b_i) \\
\mathsf{LM}\, \Phi \underline{y}^\beta \epsilon_{3i} &= \mathsf{LM}\, \underline{y}^\beta (v_i - w_i) = \mathsf{LM}\, \underline{y}^\beta v_i
\end{aligned}$$

Using Lemma 6.31 it follows that $\operatorname{Im} \widetilde{\Phi} \supseteq \mathsf{LM} \ker \widetilde{\Psi}$.

The map Φ has the normal form property, because the term orders involved are well-orders. The standard map theorem 6.10 applies, from which the results $\operatorname{Im} \Phi = \ker \Psi$ and $\operatorname{Im} \widetilde{\Phi} = \mathsf{LM} \operatorname{Im} \Phi$ follow immediately. The statement $\operatorname{Im} \widetilde{\Psi} = \mathsf{LM} \operatorname{Im} \Psi$ means that the triple $(\{h_i\}, \{f_i\}, \{g_i\})$ forms a standard basis for $\operatorname{Im} \Psi$. This completes the proof. ∎

Implementing the criterion The map $\mathrm{NF}_r^{\Psi_1}$ of Theorem 6.33 is just the normal form algorithm 6.2 for ideals. The algorithm that computes NF_r^{Ψ} is the 'union' of algorithm 6.28 for modules over subalgebras, and algorithm 6.2: For each leading term, try to write it as an ideal element and, when that fails, try to write it as an element of the subalgebra-module.

In sections 6.4.1 and 6.4.4 it is explained how to compute syzygies of the first and second kind, the s_i and b_i of Theorem 6.33. We now assume that $\{h_1, \ldots, h_k\}$ is already a standard ideal basis. This means that the $\Psi_1 s_i$ reduce to zero so that we can forget about syzygies of the first kind. It remains to find generators v_i of the $\mathbf{R}[y]$-module $\widetilde{\Psi}_2^{-1}(\mathsf{LM} \langle h_1, \ldots, h_k \rangle)$. Using the notation of section 6.4.4, this submodule is generated by the monomials in $\langle I_N \cup \{\mathsf{LM}\, h_1, \ldots, \mathsf{LM}\, h_k\} \rangle$ intersected with $\{1, t_2, \ldots, t_l\}\mathbf{R}[y]$ (here we use that $\{h_1, \ldots, h_k\}$ is a standard

basis). A possible line of attack is therefore: Compute generators of the largest monomial ideal contained in $\langle I_N \cup \{\mathsf{LM}\, h_1, \ldots, \mathsf{LM}\, h_k\}\rangle \cap \mathbf{R}[t, y]$ (which is automatically a Gröbner basis), and select the elements in $\{1, t_2, \ldots, t_l\}\mathbf{R}[y]$. With the proper term order, this amounts to one Gröbner basis calculation, and one 'inverse' Gröbner basis calculation. More precisely, this is the algorithm:

Algorithm 6.34. *(Computing syzygies $v_i - w_i$ of the third kind)*
Input: *A basis G for the ideal I_N (see Prop. 6.26), a term order $\preccurlyeq$ with $\{y_i\} \preccurlyeq \{t_i\} \preccurlyeq \{x_i\}$ which is graded in the t_i, a map Ψ with $\Psi e_{21} = f_1 = 1$, and such that $\{\Psi e_{11}, \ldots, \Psi e_{1k}\} = \{h_1, \ldots, h_k\}$ is a Gröbner basis.*
Output: *Generators $v_1, \ldots, v_r$ of the monomial ideal $\widetilde{\Psi}_2^{-1}(\langle \mathsf{LM}\, h_1, \ldots, \mathsf{LM}\, h_k\rangle)$, corresponding elements $w_1, \ldots, w_r \in R^k$ with $\widetilde{\Psi}_2 v_i = \widetilde{\Psi}_1 w_i$.*
Algorithm:

Compute Gröbner basis G' for $\langle G \cup \{\mathsf{LM}\, h_1, \ldots, \mathsf{LM}\, h_k\}\rangle$ with respect to $\preccurlyeq$.
Compute $G'' = G' \cap \{1, t_2, \ldots, t_l\}\mathbf{R}[y]$
Find basis M of largest monomial subideal contained in $\langle G''\rangle \subseteq \mathbf{R}[t, y]$
$M \leftarrow M \cap \{1, t_2, \ldots, t_l\}\mathbf{R}[y]$ and label the elements $v_1, v_2, \ldots, v_r$
For $i = 1, \ldots, r$, do the following:
    Find $m \in \mathbf{R}[x]$ and j such that $\widetilde{\Psi}_2 v_i = m\, \mathsf{LM}\, h_j$
    $w_i \leftarrow m e_{1j}$
EndFor

Proof: By the choice of term order $\preccurlyeq$, the elements in $B \cap \{1, t_2, \ldots, t_l\}\mathbf{R}[y]$ generate $\langle B\rangle \cap \{1, t_2, \ldots, t_l\}\mathbf{R}[y]$, for any Gröbner basis B, hence the output $\{v_1, \ldots, v_r\}$ is indeed a basis for the largest monomial ideal contained in $I_N \cap \{1, t_2, \ldots, t_l\}\mathbf{R}[y]$. The body of the final For-loop is simply the normal form algorithm NF^{Ψ_1} for ideals written down explicitly – it takes only one pass for monomials. ∎

Remark 6.35. *(A shortcut)* If the basis G is a Gröbner basis for I_N to start with, the computation of G' is a bit easier: Only syzygies of monomials and binomials need to be checked. The result is a monomial, and its reduction is either zero or a single new monomial.

To compute the basis M in line 3 of above algorithm, note that a monomial is in $\langle G''\rangle$ if and only if it is reduced to 0 by the ordinary normal form algorithm 6.2. The basis G'' consists of binomials and monomials only (because the S-polynomial that occur are either monomials or binomials; see [ES96, Prop. 1.1]). A reduction by a binomial results in a (nonzero) monomial, whereas a monomial reduction results in 0. Therefore, a basis for the largest monomial ideal contained in M can be found by running the normal form algorithm backwards via the binomials, starting from the monomials in G'':

Algorithm 6.36. *(Finding largest monomial subideal)*
Input*: A Gröbner basis G consisting of monomials and binomials only.*

Output: *A (Gröbner) basis M for largest monomial ideal $\langle M\rangle \subset \langle G\rangle$*
Algorithm:

$M \leftarrow$ all monomials of G
$B \leftarrow$ all binomials of G
For all monomials x^α in M, do the following:
  For all binomials $x^\beta - x^\gamma$ in B (where $x^\beta > x^\gamma$) do
    If $x^{\beta+(\alpha-\gamma)^+} \notin \langle M\rangle$, then
      Add it to M
    EndIf
  EndFor
EndFor
Output M

Here α^+, where α is a vector in $\mathbb{Z}^n$, denotes the vector α with all negative entries replaced by zeroes.

Proof: Let m be a monomial in $\langle G\rangle$. We shall prove: If m can be reduced via a $g \in G$ to m' and $m' \in \langle M\rangle$, then $m \in \langle M\rangle$. Since G is a Gröbner basis a finite number of reduction steps yield a monomial m'' which is a multiple of some monomial in G. Since M contains all monomials of G this means that that $m'' \in \langle M\rangle$, hence by 'backward induction' $m \in \langle M\rangle$.

Write $g = x^\beta - x^\gamma$ and $m = x^\delta$, and assume that $\mathsf{LM}\, g = x^\beta | m = x^\delta$, then the reduct of m by g is $x^{\delta-\beta+\gamma}$. Assume that this monomial is in $\langle M\rangle$, say $x^\alpha | x^{\delta-\beta+\gamma}$ with $x^\alpha \in M$. Using $x^\beta | x^\delta$ it follows that $x^{(\alpha-\gamma)^+} | x^{\delta-\beta}$, and after multiplication with x^β this becomes $x^{\beta+(\alpha-\gamma)^+} | x^\delta$. By the algorithm, $x^{\beta+(\alpha-\gamma)^+} \in \langle M\rangle$, hence $x^\delta \in \langle M\rangle$. ∎

Remark 6.37. *(Efficiency)* When a monomial m is added to M, it may render other monomials in M redundant, namely those that are multiples of m. The algorithm becomes a little more efficient if these are removed.

6.5 The ring of formal power series

The analogue of a Gröbner basis, in the ring of formal power series, is commonly called a *standard basis*.[3] Introduced in 1964 by Hironaka [Hir64], it preceded the notion of Gröbner basis, which was introduced by Buchberger in his thesis of 1965, see [Buc65]. Meanwhile it has been shown (see e.g. [Bec90a, Bec90b, Bec93]) that concepts in one context have close analogues in the other. The aim of this section is to show that the standard basis criteria developed above, for various subsets of the polynomial ring, have similar analogues in the ring of formal power series. Because of the modular (or 'object-oriented') set-up, we only have to show that the normal form property continues to hold.

[3] In this chapter we call such bases *standard ideal bases*, and use the term *standard basis* in the more general sense explained before.

6.5.1 Three approaches

A polynomial has finitely many terms, so whatever term order is chosen, the *leading* or highest term is well-defined. This is not so for formal power series. In that case, to guarantee existence of the leading term, the term order should be a reversed well-order, that is, every nonempty subset of terms should have a *highest* term. In this section we suppose that the term order is a reversed well-order.

Unless the number of monomials is finite, a reversed well-order is not a well-order, and the normal form algorithm 6.2 will not terminate in general, so existence of a normal form becomes an issue. There are different ways to approach this problem. Instead of looking at all ideals, one can restrict to ideals generated by *polynomials* (cf. [CLO98, p. 165]). It turns out that such ideals admit standard bases consisting of rational functions. Moreover a suitable normal form algorithm exists, acting within the ring of rational functions. This algorithm is known as the *Mora normal form*, see [Mor82, Mor85], and leads to the theory of standard ideal bases in local rings, see [GP88].

Another way of dealing with the infiniteness is to *truncate*. This makes the set of monomials finite, and hence recovers the well-ordering property of the term order. Although Mora's approach is more elegant than the method of truncation, the former only seems to work in the context of ideals. For our intended application we also need subalgebra bases, which are infinite in general, so that we need to truncate anyhow. See section 6.5.3 for more details.

A third approach is to let go of the algorithmic character altogether, and define the normal form map inductively. In this way we recover Hironaka's result that every ideal has a standard basis, see also [Bec93]. This is the subject of the next section.

6.5.2 Existence of a normal form for formal power series

In order to prove that a normal form map exists, we need some lemmas. We assume the term order is a reversed well-order.

Lemma 6.38. *Let $u \neq 1$ be a monomial, and assume u has no successor. Then there exists a strictly decreasing sequence of monomials u^i, $i \in \mathbb{N}$ such that $u = \inf_{i\in\mathbb{N}} u^i$.*

Proof: The set of monomials is countable. Let w^i be a counting of them, without duplicates, and assume $w^0 = 1$. Set $u^0 = 1$ and define

$$u^{i+1} := w^j \quad \text{with} \quad j := \min\{k | u^i > w^k > u\}.$$

(Note that $j > i$.) Each u^{i+1} is well-defined since otherwise u^i would be a successor of u. It is clear that $\{u^i\}$ is strictly decreasing. To prove that $u = \inf_i u^i$, let w^n be any monomial larger than u, then since $u^{n+1} = w^j$ for some $j > n$, this implies that $u^n \leq w^n$ by definition of u^{n+1}. ∎

The topology on the ring of formal power series $R = \mathbf{R}[[x]]$ is that of term-wise convergence. This implies that a sum of terms $\sum_i t_i$ converges if $|t_i| \to \infty$ as $i \to \infty$. Here $|\cdot|$ is the total degree: $|cx^\alpha| := \alpha_1 + \cdots + \alpha_n$. Given a map $\Psi : M \to R$, we extend the total degree function to M by setting $|m| := |\widetilde{\Psi} m|$. Now we can state the result:

Proposition 6.39. *Let $\Psi : M \to R$ be a linear map, such that the associated monomial map $\widetilde{\Psi}$ is well-defined. Assume further that M has the topology of term-wise convergence, and that Ψ is continuous. Then Ψ has the normal form property.*

Remark 6.40. By the assumption that $\widetilde{\Psi}$ is well-defined we mean that $\Psi m \neq 0$ for monomials m. Continuity of Ψ is equivalent to the statement that for any monomial $m \in R$ there are only finitely many monomials m' such that $\mathsf{LM}\, \Psi m' = m$.

For the proof we need two more results.

Lemma 6.41. *Let u^i be a strictly decreasing sequence of monomials. Then $|u^i| \to \infty$ as $i \to \infty$.*

Proof: Assume it does not, then there is an infinite, strictly decreasing subsequence $\hat{u}^i$ with $|\hat{u}^i|$ =constant, but there are only finitely many monomials with a given total degree. ∎

Theorem 6.42. *(Transfinite induction) Let P be a property of elements of a set T, and let T be well-ordered. Suppose that for all $u \in T$ we have that if $P(u')$ holds for all $u' < u$, then $P(u)$ holds. (In particular, $P(1)$ is true, where 1 is the smallest element of T.) Then $P(u)$ holds for all $u \in T$.*

Proof: [Wae60, p. 17] Suppose the set $S := \{u \in T | P(u) \text{ does not hold}\}$ is non-empty. By well-orderedness it has a smallest element, say u; in other words $P(u')$ holds for every $u' < u$. This implies, by assumption, that $P(u)$ holds, a contradiction. ∎

Proof of Proposition 6.39: Let $f \in R$ be given. Let T be the set of monomials of R, with the element $-\infty$ adjoined, which is supposed to be smaller than any monomial. Let $P(u)$, with $u \in T$, denote the following property:

$$P(u) \Leftrightarrow \begin{cases} \alpha_u \in M \text{ and } r_u \in R \text{ are well-defined,} \\ \Psi\alpha_u + r_u = f, \\ r_u = 0 \text{ or } \mathsf{LM}\, r_u \notin \operatorname{Im} \widetilde{\Psi} \text{ or } \mathsf{LM}\, r_u \leq u. \end{cases}$$

Assume $P(u')$ holds for all $u' > u$. We show that $P(u)$ also holds.

If $u = 1$, the largest element, then set $\alpha_1 := 0$ and $r_1 := f$, and $P(1)$ holds.

Suppose u has a successor $v > u$, then $P(v)$ holds. If $r_v = 0$ or $\mathsf{LM}\, r_v \notin \operatorname{Im} \widetilde{\Psi}$ or $\mathsf{LM}\, r_v \neq v$, then set $r_u := r_v$ and $\alpha_u := \alpha_v$, making $P(u)$ true. If not, then

$\mathsf{LM}\, r_v \in \operatorname{Im}\widetilde{\Psi}$, say $\mathsf{LT}\, r_v = \widetilde{\Psi} t_v$. Define $\alpha_u := \alpha_v + t_v$ and $r_u := r_v - \Psi t_v$, and $P(u)$ holds.

So suppose $u < 1$ has no successor, then by Lemma 6.38 a decreasing sequence u^i of monomials exists, with infimum u. (This is also true if $u = -\infty$.) Applying Lemma 6.41 we find $|u^i| \to \infty$. From the way the r_{u^i} are constructed, using continuity of Ψ, this implies that the sequence r_{u^i} converges. By definition of total degree on M, also $|t_{u^i}| \to \infty$. Since M has the topology of term-wise convergence, this implies convergence of α_{u^i}. Define $r_u := \lim_{i\to\infty} r_{u^i}$ and $\alpha_u := \lim_{i\to\infty} \alpha_{u^i}$. Again using continuity of Ψ we find $\Psi\alpha_u + r_u = \lim_{i\to\infty}(\Psi\alpha_{u^i} + r_{u^i}) = f$. If r_{u^i} does not become constant from some i on, we have either $r_u = 0$ or $\mathsf{LM}\, r_u \leq v$ for all $v > u$. Since u has no successor the latter inequality implies $\mathsf{LM}\, r_u \leq u$. This shows that $(\forall u' > u : P(u')) \Rightarrow P(u)$.

For the application of Theorem 6.42, reverse the ordering of the monomials. Then the order becomes a well-order (the smallest element of any set of monomials $\{t_i\}$ is $\mathsf{LM} \sum t_i$). The conclusion is that $P(u)$ holds for all $u \in T$, in particular for $u = -\infty$. Define $\mathrm{NF}^{\Psi}(f) := (\alpha_{-\infty}, r_{-\infty})$, then $P(-\infty)$ implies that this is a normal form for Ψ. ∎

Example: Standard ideal- and subalgebra-bases The statement and proofs of the theorems on standard ideal bases (Gröbner bases) and standard subideal bases in polynomial rings, remain unchanged in the present setting of formal power series. The term order is such that 1 is the largest monomial. Again the order is taken to be multiplicative, in the sense that $m_1 < m_2$ implies $mm_1 < mm_2$ for any monomial m for which multiplication is defined. Only the normal form algorithm should be replaced by the normal form map, and the word "Gröbner basis" should be replaced by "standard ideal basis". We refer to sections 6.4.1 and 6.4.3 for details.

6.5.3 Truncated formal power series

In actual computations it is not possible to work with objects that require and infinite amount of data for their description. In particular, we cannot do computations with formal power series. In Sect. 6.5 two solutions to this problem were mentioned, namely restricting to rational functions, and truncating. In this section we describe the latter in more detail.

How to truncate Let us suppose that a map $\Psi : M \to R$ has been fixed, as well as a monomial order on R, and a compatible order on M. A natural and general way of truncating is to restrict to some finite vector space generated by monomials. In this section we give a condition on this vector space R' that makes the truncation "nicely behaved".

The philosophy is as follows. Given spaces M' and R', we restrict $\Psi : M \to R$ to a map between finite dimensional vector spaces $\Psi' : M' \to R'$, by setting $\Psi' := \pi_{R'}\Psi|_{M'}$, where $\pi_{R'}$ is the canonical projection to R'. Then we want that the information contained in Ψ is also contained in the restriction of Ψ, insofar as

it pertains to the monomials in M' and R'. In more precise terms, the following seem natural conditions:

(1) $\operatorname{Im}\Psi' = \pi_{R'} \operatorname{Im}\Psi$,
(2) $(\Psi')\widetilde{\ } = (\widetilde{\Psi})'$,
(3) $\operatorname{Im}\widetilde{\Psi}' = \pi_{R'} \operatorname{Im}\widetilde{\Psi}$,
(4) Ψ is a standard map $\Rightarrow \Psi'$ is a standard map.

It is difficult to see what the weakest condition on M' and R' is, given a map Ψ, such that these conditions are fulfilled. However, a natural condition on R' and M' exists that ensures conditions (1) to (4) above, namely

$$R' := \{m | m \text{ a monomial}, m > m'\},$$
$$M' := \{m \in M | m \text{ a monomial}, \widetilde{\Psi} m \in R'\}, \tag{6.16}$$

for some monomial m'. The form of R' implies that the maps LM and $\pi_{R'}$ commute on R. This in turn implies (2) and (4). The form of M' then implies (1) and (3).

In practice the term orders are multiplicative, and a set R' is finite-dimensional and nontrivial only if the term order is a graded term order. For instance, for pure lexicographic orders the set (6.16) either is infinite-dimensional, or does not contain all variables. The vector space M' is of the same form as R', because of the compatibility of the term orders.

There is another way of describing the truncation. In the case that R is a ring, which includes all of our applications, the span of B is the quotient of R by an ideal, because of the multiplicative property of the term order. This ideal is called the *truncation ideal*. Generators of this ideal include m', but usually it is necessary to include more generators. The truncation ideal is never used in this work.

Normal form For finite sets of monomials, a total order is always a well-order. Therefore algorithms 6.13 and 6.14 terminate, which proves that the normal form property holds in the context of truncated power series, and reduced normal forms exist.